

UNITED STATES DISTRICT COURT

for the
District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

The 29 computers (including cell phones) and storage
mediums, as described in Attachment A, which are
currently in FBI custody within the District of Oregon.

Casc No. 3:25-mc-00296

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The 29 computers (including cell phones) and storage mediums, as described in Attachment A, which are currently in FBI custody within the District of Oregon.
located in the _____ District of _____ Oregon _____, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1201(c)	Conspiracy to Kidnap
18 U.S.C. § 1201(a)(1)	Kidnapping

The application is based on these facts:
See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Jaron Cookson, Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephone at 3:55 pm (specify reliable electronic means).

Date: March 14, 2025

City and state: Portland, Oregon

Jolie A. Russo
Judge's signature

Hon. Jolie A. Russo, United States Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

The property to be searched are the 29 computers¹ (including cell phones, as described below) and storage mediums which were seized on September 24, 2024, pursuant to multiple search warrants², from multiple residences and vehicles located at that time in the Middle District of Florida. The 29 computers, referred to collectively as the “**Target Devices**,” are currently in FBI custody within the District of Oregon and include the following:

1. One iPhone with a blue back, model number A2632, assigned FBI evidence number 1B59.
2. One black RIG thumb drive, model number 7HX, M/C 210301011, assigned FBI evidence number 1B60;
3. One white Xbox, serial number 007253214517, assigned FBI evidence number 1B61;
4. One white and translucent computer tower, serial number CCE4-F131-70E6-171D-9, assigned FBI evidence number 1B62;
5. One iPhone with a black back, assigned FBI evidence number 1B49.
6. One iPhone with black back, Model A1660, assigned FBI evidence number 1B50.
7. One iPhone with a cracked and black-colored back, IMEI 356830111287710, assigned FBI evidence number 1B52.
8. One black ROG Zephyrus laptop, serial number NANRKD007151404, assigned FBI evidence number 1B54.
9. One iPhone with a silver or light blue back, assigned FBI evidence number 1B55.

¹ The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media. The devices may be accessed and copied or mirrored.

² 3-24-mj-1429-MCR, 3-24-mj-1430-MCR, 3-24-mj-1434-MCR, 3-24-mj-1435-MCR, 3-24-mj-1428-MCR, 3-24-mj-1432-MCR, 3-24-mj-1433-MCR.

10. One iPhone with a black back, Model A1660, assigned FBI evidence number 1B51.
11. One white Logitech thumb drive, model G733, FCCID JNZA00080, assigned FBI evidence number 1B53.
12. One HP Omen 30 L Desktop PC, serial number 2M021458GF, assigned FBI evidence number 1B56.
13. One iPhone with a black case, assigned FBI evidence number 1B88.
14. One white Toyota card with a removable chip, assigned FBI evidence number 1B105.
15. One iPhone with a cracked and silver back, assigned FBI evidence number 1B92.
16. One black laptop with two missing keys, serial number NANRKD001159405, assigned FBI evidence number 1B95.
17. One black Skytech Gaming computer, serial number ST-473926989, assigned FBI evidence number 1B96.
18. One iPhone with a red back, assigned FBI evidence number 1B99.
19. One iPhone with a black back, assigned FBI evidence number 1B100.
20. One iPhone with a red back, assigned FBI evidence number 1B67.
21. One iPhone with a cracked blue back, assigned FBI evidence number 1B68.
22. One iPhone with a black back, assigned FBI evidence number 1B69.
23. One iPhone with a red back, assigned FBI evidence number 1B70.
24. One iPhone with a black back, assigned FBI evidence number 1B71.
25. One iPhone with a gold back and found inside a black case, assigned FBI evidence number 1B74.
26. One silver Apple Mac Book, serial number C02J9EZHQ6L4, assigned FBI evidence number 1B75.
27. One blue and gray Memorex 16GB USB, assigned FBI evidence number 1B80.
28. One black Dell laptop, service tag (S/N) C2322N2, assigned FBI evidence number 1B85.
29. One iPhone with tan or gold back, assigned FBI evidence number 1B86.

ATTACHMENT B

Particular Things to Be Seized

1. The items to be searched for, seized, and examined, are the 29 computers (including cell phones, as defined below) and storage mediums described in Attachment A and referred to collectively hereinafter as the “**Target Devices**,” which are currently in the FBI’s custody within the District of Oregon, and which contain evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 1201(c), Conspiracy to Kidnap; and 18 U.S.C. § 1201(a)(1), Kidnapping (collectively referred to as the “Target Offenses”). These items can be searched whether or not they are stored in property packaging, are in any container or safe, or are locked or unlocked. The FBI is authorized to search for, seize, and examine the following information from September 24, 2023, through the date of execution of the warrant.

2. The items to be seized pursuant to this warrant includes records, communications (e.g., “chat messages”), images, videos, contacts, financial information, and other information that are contraband, fruits of a crime, or other items illegally possessed, property designed for use, intended for use, or used in committing a crime, or that relate to or constitute evidence and instrumentalities of violations of the Target Offenses, including the following:

3. Images, videos, etc., of clothing worn by Billy Cordova (“CORDOVA”), Ralph Moreno Jr. (“MORENO”), Justice Del Carpio (“DEL CARPIO”), and/or Jackson Reves (“REVES”), referred to collectively as the **Target Suspects**, as observed by investigators around the time of the Target Offenses.

4. All communications, records, documents, programs, applications or materials related to the planning, coordination, or completion of the kidnapping and/or extortion of the adult victim (“AV”) described in the affidavit supporting this warrant, in violation of the Target

Attachment B

Offenses, including communications (e.g., “chat messages”), images, and videos that, based on training and experience, appear consistent with conspiring to commit fraudulent account takeovers or other similar criminal activity against multiple presumed victims, the relevance of which is detailed in the supporting affidavit.

5. All communications, records, documents, programs, applications or materials related to locations or identities of individuals involved in the Target Offenses.

6. All communications that investigators believe is with or about AV, whether or not his/her true name is used.

7. Records and information containing photographs, videos, and/or audio recordings related to the Target Offenses.

8. All communications, records, documents, programs, applications or materials related to bank accounts or cryptocurrency accounts/wallets used in furtherance of, or proceeds gained through the execution of, the Target Offenses (e.g., records of payments made to purchase airline tickets, cryptocurrency payments between suspected co-conspirators around the time of the Target Offenses, wallet addresses associated with these transactions, etc.).

9. Records and information about any social media, email, or other internet accounts that have been used on any seized computer, including content stored within any application contained on the device.

10. Any and all cryptocurrency, to include the following:

- a. cryptocurrency hardware wallets, digital offline storage devices, cold storage devices, Mnemonic phrases, passwords, encryption keys and seed recovery lists;
- b. any and all representations of cryptocurrency public keys or addresses, whether in electronic or physical format;

- c. any and all representations of cryptocurrency private keys, whether in electronic or physical format;
- d. any and all representations of cryptocurrency wallets or their constitutive parts, whether in electronic or physical format, to include “recovery seeds” or “root keys” which may be used to regenerate a wallet;
- e. PGP keys and/or encryption passwords or keys of any kind.

11. The United States is authorized to seize any and all cryptocurrency by transferring the full account balance in each wallet to a public cryptocurrency address controlled by the United States.

12. The United States is further authorized to copy any wallet files and restore them onto computers controlled by the United States. By restoring the wallets on its own computers, the United States will continue to collect cryptocurrency transferred into the defendant’s wallets as a result of transactions that were not yet completed at the time that the defendant’s devices were seized.

13. Evidence of who used, owned, or controlled any computer or storage medium at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chats,” instant messaging logs, photographs, and correspondence;

14. Evidence of software that would allow others to control any seized computer or storage medium, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software, and evidence of the lack of such malicious software.

15. Evidence indicating how and when any computer or storage medium was accessed or used to determine the chronological context of access, use, and events relating to Target Offenses and to the user(s).
16. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from any seized computer.
17. Evidence of the times any seized computer was used.
18. Passwords, encryption keys, and other access devices that may be necessary to access any seized computer.
19. Records and information about any seized computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
20. Contextual information necessary to understand the evidence described in this attachment.
21. Routers, modems, and network equipment used to connect computers to the Internet.

DEFINITIONS

22. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

///

23. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

24. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

SEARCH PROCEDURES

25. All evidence is to be seized for the time period from September 24, 2023, through the date of execution of the warrant, except that attribution evidence may be for any period of time through the date of the execution of the warrant.

26. The examination of the computers and storage mediums described herein may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the computers or storage mediums to human inspection in order to determine whether it is evidence described by the warrant.

27. The initial examination of the computers or storage mediums will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

///

28. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computers or storage mediums or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

29. If an examination is conducted, and it is determined that a computer or storage medium does not contain any data falling within the ambit of the warrant, the government will return the computers or storage mediums to its owner within a reasonable period of time following the search and will seal any image of the computer or storage medium, absent further authorization from the Court.

30. The government may retain the computers or storage mediums as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computers or storage mediums and/or the data contained therein.

31. The government will retain a forensic image of the computers or storage mediums for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

DISTRICT OF OREGON, ss:

AFFIDAVIT OF JARON T. COOKSON

**Affidavit in Support of an Application Under Rule 41
for a Warrant to Search Digital Evidence**

I, Jaron T. Cookson, being duly sworn, do hereby depose and state as follows:

Introduction and Identity of Affiant

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been so employed since March 2020. I was assigned to the Portland Division’s Cyber squad until March 9, 2025, at which time I transitioned to the Charlotte Division’s Cyber squad. I have over thirty months of prior experience on Portland’s Violent Gang squad. In December 2020, I successfully completed the twenty-week New Agent’s Training course at the FBI Academy in Quantico, Virginia. During that time, I was taught how to investigate multiple criminal violations including cyber-based offenses. Since becoming a Special Agent, I have been responsible for and actively participated in numerous investigations for which I used a variety of investigative techniques, including interviewing witnesses and subjects of investigations; serving subpoenas and analyzing the documents obtained thereby; preparing and executing search and arrest warrants; analyzing financial records, public records, social media, and content stored on electronic devices; conducting surveillance; and the use of confidential human sources. Through my training and experience, I have become familiar with how members of a criminal enterprise communicate and use electronic communications to store, transmit, and distribute information to one another. As a federal agent, I am authorized to investigate and enforce violations of the criminal laws set forth in Titles 18 and 21 of the United States Code.

///

///

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the 29 computers¹ and storage mediums detailed below and in Attachment A for digital evidence. These computers and storage mediums (also referred to herein as the “**Target Devices**”) were initially seized on September 24, 2024, from residences and vehicles in Florida, pursuant to warrants signed by the Honorable Monte C. Richardson, United States Magistrate Judge, Middle District of Florida. Those warrants required the initial examination of the **Target Devices** to occur within 120 days from the execution of the warrant, which has expired, and the completed review within 180 days, which is upcoming. In addition, since their initial seizure, the **Target Devices** were transported to the District of Oregon, where they are currently in FBI custody. As such, this application seeks a new warrant, now from the District of Oregon, to search the **Target Devices** detailed below and in Attachment A for evidence, as described in Attachment B.

3. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1201(c), Conspiracy to Kidnap; and 18 U.S.C. § 1201(a)(1), Kidnapping (“**Target Offenses**”), were committed by Billy Cordova (“**CORDOVA**”), Ralph Moreno Jr. (“**MORENO**”), Justice Del Carpio (“**DEL CARPIO**”) and Jackson Reves (“**REVES**”), referred to collectively as the **Target Suspects**, and that evidence of the Target Offenses is located on the devices seized from their residences and/or vehicles, as detailed below. As such, I believe there is also probable cause to search the information described in Attachment A for evidence of the Target Offenses as further described in Attachment B.

¹ The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media. The devices may be accessed and copied or mirrored

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Target Offenses

5. I believe there is probable cause that evidence of the following violations will be found in the places to be searched:

- 18 U.S.C. § 1201 provides, in part:

(a) Whoever unlawfully seizes, confines, inveigles, decoys, kidnaps, abducts, or carries away and holds for ransom or reward or otherwise any person, except in the case of a minor by the parent thereof, when—

(1) the person is willfully transported in interstate or foreign commerce, regardless of whether the person was alive when transported across a State boundary, or the offender travels in interstate or foreign commerce [. . .] in committing or in furtherance of the commission of the offense.

...

(c) If two or more persons conspire to violate this section and one or more of such persons do any overt act to effect the object of the conspiracy, each shall be punished by imprisonment for any term of years or for life.

STATEMENT OF PROBABLE CAUSE

6. Since November 2023, the FBI Portland Division has been investigating the kidnapping of the Oregon resident referred to herein as D.J.J. In summary, on November 10, 2023, D.J.J. was kidnapped from outside of his Portland, Oregon apartment. D.J.J. was assaulted and robbed of cryptocurrency until early the next morning (November 11, 2023), when he was

Affidavit of Jaron T. Cookson **Page 3**

left bound to a post in an empty field in North Plains, Oregon. A passer-by found D.J.J. still bound to the post later that morning and contacted law enforcement. D.J.J. was transported to the hospital and treated for numerous injuries, including right pneumothorax (i.e., collapsed lung), multiple fractured ribs, and multiple fractured fingers, among other ailments. Investigators believe D.J.J. was targeted because of his past engagement in criminal activity, to include “SIM swapping”² and wire fraud violations involving the theft of millions of dollars of cryptocurrency. D.J.J. may have also been targeted because of a renewed engagement in criminal activity at the time of his kidnapping, as detailed below.

7. Investigators identified at least four Florida residents who conspired together to conduct the kidnapping and extortion: CORDOVA, MORENO, DEL CARPIO, and REVES (“**Target Suspects**”). On September 10, 2024, a sealed indictment was filed against the **Target**

² Based on my training and experience, and conversations with other investigators, I have learned the following:

(1) A Subscriber Identity Module (hereinafter “SIM”) card is a removable and separately purchasable electronic card within a cellular device that stores user data in Global System for Mobile (GSM) phones and directs wireless transmissions to specific phones. Without a SIM card, a GSM cellular phone would not be authorized to use a mobile network except to make calls to emergency services.

(2) A SIM swap scam is a fraud that occurs when a fraudster activates a new SIM card and redirects – or *ports* – the victim’s telephone number to a device within the fraudster’s control. Once the fraudster gains access and control over the victim’s cellular phone, the fraudster(s) can then access the phone communications, in particular Short Message Service (hereinafter “SMS”) text messages. The fraudster is then able to take advantage of a weakness in two-factor authentication and verification in which the second step is an SMS text message or call to the victim’s cellular phone number. As such, the fraudster will receive any codes and passwords/password reset requests sent to that phone via call or text for any accounts accessible on the mobile device. After receiving the password or password reset link for an account, the fraudster will gain access to that account, change the password to lock out the legitimate user, then steal any available funds from financial applications used by the legitimate owner of those funds.

(3) Individuals will often coordinate criminal efforts with other fraudsters to effectuate a SIM swap attack and will assume specific roles within the scheme. For example, one person may find viable targets, another person may conduct social engineering attacks against a phone provider, another may develop malicious software to deploy against the phone providers, and others may perform money laundering activities to turn their illicit proceeds into fiat currency. Depending on the crew and specific circumstances of any given SIM swap scam, different attacker roles may be required. Individuals conspiring to commit these crimes are most often located in different states and often in different countries. They communicate over the internet and often use Telegram to communicate.

Suspects in the United States District Court for the District of Oregon. The **Target Suspects** were charged in that indictment for violating the Target Offenses, and arrest warrants were issued.

8. On September 23, 2024, Judge Richardson, Middle District of Florida, signed multiple warrants authorizing the search of four locations (“Target Locations”) where the **Target Suspects** were believed to reside.³ The warrants also authorized the search of three vehicles (“Target Vehicles”) which the **Target Suspects** were believed to used.⁴ That application and its supporting affidavit, which are attached hereto as Exhibit 1, established probable cause that evidence of the **Target Suspects**’ knowledge and/or participation in the Target Offenses would be located where the **Target Suspects** resided and in the vehicles they regularly used. The Target Locations and Target Vehicles were located in the Middle District of Florida and included the following:

- i. 20 Blackwell Pl, Palm Coast, Florida 32137;
- ii. 5000 Yukon Dr, Unit 308, Palm Coast, Florida 32137;
- iii. 6 Flemington Ln, Palm Coast, Florida 32137;
- iv. 116 Red Mill Dr, Palm Coast, Florida 32164;
- v. Silver 1998 Honda Civic bearing Florida license plate IQ13HJ, VIN:
1HGEJ8147WL075628;
- vi. White 2020 Dodge Charger bearing Florida license plate 25BJAN, VIN:
2C3CDXHG2LH186169;

///

³ 3-24-mj-1429-MCR, 3-24-mj-1430-MCR, 3-24-mj-1434-MCR, 3-24-mj-1435-MCR

⁴ 3-24-mj-1428-MCR, 3-24-mj-1432-MCR, 3-24-mj-1433-MCR

- vii. Black 2019 Toyota Camry bearing Florida license plate QFKG23, VIN:
4T1BZ1HK7KU026287.

9. The evidence investigators were authorized to search, seize, and examine pursuant to the foregoing warrants included the computers (as defined above, and including cell phones) and electronic storage mediums specifically used by the **Target Suspects**, and capable of storing encrypted communications (e.g., Telegram), cryptocurrency (e.g., cryptocurrency allegedly stolen from D.J.J.), and/or other digital evidence of the Target Offenses (e.g. stored media, seed phrases, and QR codes for cryptocurrency wallets⁵). Because the warrants authorized the search of computers used by the **Target Suspects** and not potential cohabitants, the warrants required investigators to obtain additional evidence that the computer or storage medium was used by the specific **Target Suspect** who was believed to reside at the Target Location or believed to use the Target Vehicle where the evidence was found. Such additional evidence included but was not limited to:

- i. Locating the computer or storage medium in a bedroom with indicia of the **Target Suspect**⁶ as an occupant of that room (e.g., mail in the room with the **Target Suspect's** name; clothing in the room that appears consistent in size and/or appearance with clothing worn by the **Target Suspect** as observed by investigators; identification cards, etc.);

///

///

⁵ The terms “seed phrases” and “cryptocurrency wallets” refer to methods for storing and accessing cryptocurrency.

⁶ To simplify this summary, I am grouping the **Target Suspects** together in this list; however, as detailed in the previous paragraph and in Exhibit 1, the warrant applied only to the specific **Target Suspect** associated with the Target Location and/or Target Vehicle where the evidence was located.

- ii. Statements made by the **Target Suspect** or another occupant of the Target Location indicating the computer or storage medium was owned and/or used by the **Target Suspect**;
- iii. Evidence that the **Target Suspect** appeared to be the sole occupant of the Target Location or primary operator of the Target Vehicle;
- iv. Indicia of the **Target Suspects'** ownership or operation of the device (e.g., account names on the computer or storage medium, images related to the **Target Suspect** on the computer's background, etc.) found during a preliminary review of the device conducted for that purpose;

10. Search warrants issued in the District of Oregon typically contain search procedures that provide certain time limitations for reviewing digital evidence on electronic devices, which are detailed in the respective warrant's Attachment B. These limitations require the initial examination of electronic devices to occur within 120 days from the execution of the warrant and the completed review within 180 days. These procedures were added into the Florida warrants as the cases would ultimately be prosecuted in the district of Oregon. Per conversations with an AUSA in the Middle District of Florida, it is not their typical practice to include similar time limitations in the Attachment B for their warrants to search digital evidence.

11. On September 24, 2024, the FBI and its assisting agencies arrested the four **Target Suspects** at the four Target Locations. The FBI and its assisting agencies then completed a search of the Target Locations and Target Vehicles, during which numerous items of evidence were seized, including the **Target Devices**. The **Target Devices** were eventually transported to the District of Oregon where, as of the date of this application, they are in FBI custody in Oregon. Investigators started the initial examination of multiple **Target Devices**, but not all.

Moreover, due to the number of devices and total volume of content, investigators have not completed the review of any **Target Device**. As such, this application seeks a new warrant from the District of Oregon to search of these **Target Devices**.

12. In addition, while reviewing the **Target Devices** for which the initial examination had started prior to the 120-day expiration, investigators observed numerous “chat” messages in plain view that, based on training and experience, appeared consistent with conspiring to commit fraudulent account takeovers against multiple presumed victims. Based on my training and experience, and my knowledge of the investigation to date, I believe this language is relevant to the planning, coordination, and/or completion of the kidnapping and extortion of D.J.J. As detailed in Exhibit 1, D.J.J. was previously involved in similar criminal activity. Such communications are relevant to show the **Target Suspects’** potential knowledge of D.J.J. prior to the Target Offenses, as well as D.J.J.’s past possession of millions of dollars in criminal proceeds, which D.J.J. alleged was a motive for his extortion. As such, Attachment B has been updated from the original warrant to specifically include language specifically authorizing the seizure of such communications, pursuant to this warrant.

13. As stated above, the warrants required investigators to obtain additional evidence that the computer or storage medium was used by the specific **Target Suspect** who was believed to reside at the Target Location or use the Target Vehicle where the evidence was found. Detailed below are the locations from which the **Target Devices** were seized and some of the observations made by investigators leading to my belief that the **Target Devices** were likely owned and/or operated by the **Target Suspects**.

///

///

CORDOVA's Residence, 20 Blackwell Pl, Palm Coast, Florida

14. During the search of 20 Blackwell Pl, Palm Coast, Florida ("20 Blackwell"), investigators interviewed one of the occupants of 20 Blackwell (hereinafter "Cohabitant-1").⁷ Cohabitant-1 identified CORDOVA's bedroom, which investigators subsequently labeled "Room E." Investigators also located multiple articles of clothing inside Room E consistent with clothing that investigators previously observed CORDOVA wearing. As such, investigators determined Room E was CORDOVA's personal bedroom and thus the electronic devices located in Room E were likely owned and/or operated by CORDOVA. The following devices were seized from Room E during the search.

- i. One iPhone with a blue back, model number A2632, located on the ottoman at the foot of the bed in Room E and assigned FBI evidence number 1B59. Investigators started but have not completed the review of the initial cellphone extraction.
- ii. One black RIG thumb drive, model number 7HX, M/C 210301011, located on top of the dresser in Room E and assigned FBI evidence number 1B60.
- iii. One white Xbox, serial number 007253214517, located on the dresser in Room E and assigned FBI evidence number 1B61.
- iv. One white and translucent computer tower, serial number CCE4-F131-70E6-171D-9, located next to the desk in Room E and assigned FBI evidence number 1B62.

MORENO's Residence, 5000 Yukon Dr, Unit 308, Palm Coast, Florida

15. During the search of 5000 Yukon Dr, Unit 308, Palm Coast, Florida ("5000 Yukon"), investigators interviewed one of the occupants of 5000 Yukon (hereinafter

⁷ The identities of the unnamed cohabitants identified herein are known to investigators but are obfuscated herein to shield their identity.

“Cohabitant-2”). Cohabitant-2 confirmed he/she and MORENO were the only occupants of 5000 Yukon at that time. When asked what bedroom was MORENO’s, Cohabitant-2 said it would be obvious because Cohabitant-2’s room was orderly but MORENO’s room was in disarray and still had moving boxes in it. Cohabitant-2 also confirmed he/she only possessed one cell phone inside the apartment, and it was located on the nightstand in Cohabitant-2’s bedroom (later labeled “Room F”). According to Cohabitant-2, all other devices located in 5000 Yukon belonged to MORENO. Cohabitant-2 was later allowed to retrieve his/her phone, thus according to Cohabitant-2 all remaining devices located thereafter belonged to MORENO. When investigators searched 5000 Yukon, Room F appeared orderly whereas the other bedroom, later labeled “Room E,” appeared to be in disarray and had “The Home Depot” boxes on the floor with items still inside. While searching Room E, investigators located multiple items indicating Room E was occupied by MORENO, including: MORENO’s Florida driver’s license and multiple pairs of shoes consistent in style and color with shoes that investigators previously observed MORENO wearing. As such, investigators determined Room E was MORENO’s personal bedroom and thus the electronic devices located inside of Room E were likely owned and/or operated by MORENO. The following devices were seized from inside Room E during the search:

- i. One iPhone with a black back, located on the rug in Room E and assigned FBI evidence number 1B49.
- ii. One iPhone with black back, Model A1660, located on the rug and near the bed in Room E; assigned FBI evidence number 1B50.
- iii. One iPhone with a cracked and black-colored back, IMEI 356830111287710, located on the bed in Room E and assigned FBI evidence number 1B52.

- iv. One black ROG Zephyrus laptop, serial number NANRKD007151404, located on the bed in Room E and assigned FBI evidence number 1B54.

16. In addition, investigators also located a cell phone on the television stand in the living room, later labeled “Room A.” The phone was locked but had multiple notifications visible on the lock screen, including an Instagram notification to the account “drugcoast.” Based on the evidence set forth in Exhibit 1 (*see* attached), investigators believe MORENO was the primary operator of the Instagram account drugcoast. On the floor immediately below the phone was a pair of white Nike shoes that were size 8.5 in Men’s. They were also consistent in style and color with shoes that investigators previously observed MORENO wearing and with multiple pairs of shoes located in Room E. In addition, as stated above, Cohabitant-2 told investigators all devices other than his/her personal phone were MORENO’s. As such, investigators believe the phone was owned and/or operated by MORENO. The phone was an iPhone with a silver or light blue back and was assigned FBI evidence number 1B55. Investigators started but have not completed the review of the initial cellphone extraction.

17. Finally, investigators also located a backpack on a chair in the dining area, later labeled “Room B.” Investigators located an iPhone and a thumb drive inside the backpack. Since Cohabitant-2 denied ownership of any additional cellphones, and said all other cellphones were MORENO’s, investigators concluded the devices located inside the backpack were likely owned and/or used by MORENO. The following devices were seized from inside the backpack:

- i. One iPhone with a black back, Model A1660, located inside the backpack on a chair in Room B and assigned FBI evidence number 1B51.

///

///

- ii. One white Logitech thumb drive, model G733, FCCID JNZA00080, located inside the front pocket of the backpack in Room B and assigned FBI evidence number 1B53.

MORENO's vehicle, a white 2020 Dodge Charger, Florida license plate 25BJAN, VIN: 2C3CDXHG2LH186169

18. At the time investigators executed the search and arrest warrants at 5000 Yukon, a white 2020 Dodge Charger bearing Florida license plate 25BJAN, VIN: 2C3CDXHG2LH186169 (hereinafter "Charger") was parked near the stairwell to 5000 Yukon. As documented in Exhibit 1 (*see attached*), Florida Driver and Vehicle Information Database ("DAVID") previously identified MORENO as the Registered Owner for the Charger. Investigators also previously observed MORENO driving the Charger on numerous occasions leading up to the search and arrest operation. In addition, during the aforementioned interview with Cohabitant-2, Cohabitant-2 indicated the Charger belonged to MORENO. As such, investigators determined the electronic devices located inside of the vehicle were likely owned and/or operated by MORENO.

- i. One HP Omen 30 L Desktop PC, serial number 2M021458GF, located in the trunk of the vehicle labeled Room I and assigned FBI evidence number 1B56.

DEL CARPIO's location, 6 Flemington Ln, Palm Coast, Florida

19. Immediately prior to DEL CARPIO's arrest at 6 Flemington Ln, Palm Coast, Florida ("6 Flemington"), FBI SWAT observed DEL CARPIO inside the room which was later labeled "Room E." DEL CARPIO appeared to be using a computer inside Room E until the FBI initiated a call-out and attempted to prevent DEL CARPIO from encrypting his computer or destroying any digital evidence. DEL CARPIO fled deeper into the house and took a cell phone

with him. DEL CARPIO was eventually arrested while still inside 6 Flemington and the cell phone was seized from his person at that time. Also on DEL CARPIO's person was a wallet with DEL CARPIO's Florida driver's license and various cards bearing his name. One of the cards was labeled "Treasure Coast Toyota of Stuart" and included a removable chip potentially capable of storing information ("Toyota chip"). As such, investigators believe the cellphone and Toyota chip were both owned and/or operated by DEL CARPIO. More specifically these items were:

- i. One iPhone with a black case, located on DEL CARPIO's person and placed on a counter in the laundry room, later labeled "Room D," from which it was later seized and assigned FBI evidence number 1B88. Investigators started but have not completed the review of the cellphone extraction.
- ii. One white Toyota card with a removable chip ("Toyota chip"), located in DEL CARPIO's wallet and later seized from Room D; assigned FBI evidence number 1B105.

20. During the search of Room E (the room in which DEL CARPIO was initially identified), investigators also located a black "The North Face" bag and multiple articles of clothing consistent with a bag and clothing DEL CARPIO was previously observed carrying and wearing. In addition, following his arrest and being advised of his Miranda rights, DEL CARPIO signed the FBI Advice of Rights form and acknowledged he understood his rights. DEL CARPIO then confirmed to law enforcement that he lived with his great grandmother, who investigators understood to be the other occupant of 6 Flemington that was present at the time of the warrant. DEL CARPIO later invoked his right to an attorney and was not asked further questions. As such, investigators determined Room E was DEL CARPIO's personal bedroom

and thus the electronic devices located inside of Room E were likely owned and/or operated by DEL CARPIO. The following devices were seized from Room E:

- i. One iPhone with a cracked and silver back, located on the white desk in Room E and assigned FBI evidence number 1B92.. Investigators started but have not completed the review of the cellphone extraction.
- ii. One black laptop with two missing keys, serial number NANRKD001159405, located on the white desk in Room E and assigned FBI evidence number 1B95.
- iii. One black Skytech Gaming computer, serial number ST-473926989, located on the white desk in Room E and assigned FBI evidence number 1B96.

DEL CARPIO's vehicle, a black 2019 Toyota Camry, Florida license plate QFKG23, VIN: 4T1BZ1HK7KU026287

21. At the time investigators executed the warrants at 6 Flemington, a black 2019 Toyota Camry, Florida license plate QFKG23, VIN: 4T1BZ1HK7KU026287, was parked in the driveway (hereinafter "Camry"). As documented in Exhibit 1 (*see* attached), DAVID listed the Camry as registered to DEL CARPIO and Shirley E Gutierrez. Investigators also previously observed DEL CARPIO driving the Camry on numerous occasions leading up to the search and arrest operation (*see* Exhibit 1). In addition, after singing the FBI Advice of Rights form, and before invoking his right to an attorney, DEL CARPIO told investigators the Camry in the driveway was his car. As such, investigators determined the electronic devices located inside of the vehicle were likely owned and/or operated by DEL CARPIO. The following items were seized from the Camry:

- i. One iPhone with a red back, located in the front passenger door (the area labeled "Quadrant B") and assigned FBI evidence number 1B99.

- ii. One iPhone with a black back, located in the front middle console (the area labeled “Quadrant A”) and assigned FBI evidence number 1B100.

REVES’ location, 116 Red Mill Dr, Palm Coast, Florida

22. Following REVES’ arrest at 116 Red Mill Dr, Palm Coast, Florida (“116 Red Mill”), investigators advised REVES of his Miranda rights. REVES stated he understood his rights but was not willing to sign the FBI Advice of Rights form and was not willing to waive his rights. Investigators then told REVES’ he would appear before a Federal Magistrate Judge later that day and was asked if there was specific clothing the FBI could retrieve for REVES. REVES’ was escorted through 116 Red Mill and he led investigators to the bedroom subsequently labeled “Room D.” While inside Room D, REVES requested a white shirt that was located on the top shelf of the closet inside of Room D. He also requested black shoes and a pair of jeans. Later during the same search, investigators located REVES’ birth certificate, Florida driver’s license, and social security card in the closet in Room D. Investigators later located a hole in the wall behind the door and inside Room D. Inside the wall, below the hole, they located a cellphone that rang when investigators called the phone number 386-569-5791. Based on the investigation (*see* Exhibit 1), investigators knew that was the phone number used by REVES. As such, investigators determined Room D was REVES’ personal bedroom and thus the electronic devices located inside Room D were likely owned and/or operated by REVES. The following devices were seized from inside Room D during the search:

- i. One iPhone with a red back, located in a box in the closet inside Room D and assigned FBI evidence number 1B67.
- ii. One iPhone with a cracked blue back, located in a box in the closet inside Room D and assigned FBI evidence number 1B68.

- iii. One iPhone with a black back, located in a box in the closet inside Room D and assigned FBI evidence number 1B69.
- iv. One iPhone with a red back, located in a box in the closet inside Room D and assigned FBI evidence number 1B70.
- v. One iPhone with a black back, located on the white desk in Room D and assigned FBI evidence number 1B71.
- vi. One iPhone with a gold back and found inside a black case, located on the nightstand next to the bed in Room D and assigned FBI evidence number 1B74.
- vii. One silver Apple Mac Book, serial number C02J9EZHQ6L4, located on the top of the shelving unit next to the bedroom door in Room D and assigned FBI evidence number 1B75.
- viii. One blue and gray Memorex 16GB USB, located in of a red container in the closet in Room D and assigned FBI evidence number 1B80.
- ix. One black Dell laptop, service tag (S/N) C2322N2, located underneath the mattress in Room D and assigned FBI evidence number 1B85.
- x. One iPhone with tan or gold back and found inside of a case, located inside the wall behind the door in Room D and assigned FBI evidence number 1B86. Investigators started but have not completed the review of the cellphone extraction.

23. Based on the facts set forth in this affidavit, and those detailed in Exhibit 1, I believe there is probable cause that violations of the Target Offenses were committed by the **Target Suspects**, and that evidence of the Target Offenses is located on the **Target Devices** which were seized from their residences and/or vehicles, as detailed above. As such, I believe

///

there is also probable cause to search the information described in Attachment A in the District of Oregon for evidence of the Target Offenses as further described in Attachment B.


CONCLUSION

24. Based on the foregoing, I have probable cause to believe, and I do believe, that the **Target Devices** described in Attachment A contains evidence of the Target Offenses, as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the **Target Devices** described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found. I further request that the Court authorize execution of the warrant at any time of day or night.

25. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Parakram Singh, and AUSA Singh advised me that in his opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant and that the information likely to be obtained is relevant to an ongoing criminal investigation.

By phone pursuant to Fed. R. Crim. P. 4.1
Jaron T. Cookson
Federal Bureau of Investigation

Subscribed and sworn by telephone in accordance with Fed. R. Crim. P. 4.1 at
3:55 pm on March 14, 2025.



HONORABLE JOLIE A. RUSSO
United States Magistrate Judge

UNITED STATES DISTRICT COURT

for the
Middle District of Florida

I CERTIFY THE FOREGOING TO BE A TRUE
AND CORRECT COPY OF THE ORIGINAL
CLERK OF COURT
UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
BY: [Signature]
DEPUTY CLERK

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Electronically Stored Information, further described in
Attachment A-8

Case No. 3:24-mj- 1431-MCR

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
Electronically Stored Information, further described in Attachment A-8,

located in the Middle District of Florida, there is now concealed (identify the person or describe the property to be seized):
see Attachment B-8.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1201(c), 18 U.S.C. § 1201(a)(1)	conspiracy to kidnap, kidnapping

The application is based on these facts:
See attached affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[Signature]
Applicant's signature

Jaron T. Cookson, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 9/23/24

City and state: Jacksonville, FL

[Signature]
Judge's signature

Monte C. Richardson, U.S. Magistrate Judge
Printed name and title

MIDDLE DISTRICT OF FLORIDA, ss: AFFIDAVIT OF JARON T. COOKSON

**Affidavit in Support of an Application
Under Rule 41 for a Search Warrant**

I, Jaron T. Cookson, being duly sworn, do hereby depose and state as follows:

Introduction and Identity of Affiant

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since March 2020. I am currently assigned to the Portland Division's Cyber squad and have over thirty months of prior experience on Portland's Violent Gang squad. In December 2020, I successfully completed the twenty-week New Agent's Training course at the FBI Academy in Quantico, Virginia. During that time, I was taught how to investigate multiple criminal violations including cyber-based offenses. Since becoming a Special Agent, I have been responsible for and actively participated in numerous investigations for which I used a variety of investigative techniques, including interviewing witnesses and subjects of investigations; serving subpoenas and analyzing the documents obtained thereby; preparing and executing search and arrest warrants; analyzing financial records, public records, social media, and content stored on electronic devices; conducting surveillance; and the use of confidential human sources. Through my training and experience, I have become familiar with how members of a criminal enterprise communicate and use electronic communications to store, transmit, and distribute information to one another. As a federal agent, I am authorized to

Affidavit of Jaron T. Cookson

Page 1

investigate and enforce violations of the criminal laws set forth in Titles 18 and 21 of the United States Code.

2. Since November 2023, I have been investigating the kidnapping of the Oregon resident referred to herein as D.J.J. As detailed below, on November 10, 2023, D.J.J. was kidnapped, assaulted, and robbed of cryptocurrency. I believe D.J.J. was targeted because of his past engagement in criminal activity, to include “SIM swapping” (detailed below) and wire fraud violations involving the theft of millions of dollars of cryptocurrency. D.J.J. may have also been targeted because of a renewed engagement in criminal activity at the time of his kidnapping, as detailed below.

3. I have since identified four co-conspirators involved in the kidnapping: Billy Shane Cordova (“CORDOVA”), Ralph Santiago Moreno Jr. (“MORENO”), Justice Uallah Del Carpio (“DEL CARPIO”) and Jackson Suha Reves (“REVES”), referred to collectively as the **Target Suspects**. On September 10, 2024, a sealed indictment was filed against the **Target Suspects** in the United States District Court for the District of Oregon. The **Target Suspects** were charged for violating 18 U.S.C. § 1201(c), Conspiracy to Kidnap; and 18 U.S.C. § 1201(a)(1), Kidnapping (“Target Offenses”), and are currently the subjects of arrest warrants.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that evidence of the **Target Suspects’** knowledge and/or participation in the Target Offenses will be located where the **Target Suspects** reside and in the vehicles

they regularly use. Such evidence includes the computers¹ (including cell phones) and electronic storage mediums specifically used by the **Target Suspects**, and capable of storing encrypted communications (e.g., Telegram), cryptocurrency (e.g., cryptocurrency allegedly stolen from D.J.J.), and/or other digital evidence of the Target Offenses (e.g. stored media, seed phrases, and QR codes for cryptocurrency wallets²). Evidence in these locations also includes clothing observed around the time of the Target Offenses. As such, this application seeks warrants to search the **Target Suspects'** residences, vehicles, and electronically stored information.

Requested Search Warrants

5. I submit this affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the following premises located in the Middle District of Florida (collectively referred to as the "**Target Residences**");

- i. 20 Blackwell Pl, Palm Coast, Florida 32137, as described in Attachment A-1 ("**CORDOVA Residence**");
- ii. 5000 Yukon Dr, Unit 308, Palm Coast, Florida 32137, as described in Attachment A-2 ("**MORENO Residence**");

¹ The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media. The devices may be accessed and copied or mirrored.

² The terms "seed phrases" and "cryptocurrency wallets" refer to methods for storing and accessing cryptocurrency.

- iii. 6 Flemington Ln, Palm Coast, Florida 32137, as described in Attachment A-3 ("**DEL CARPIO Residence**");
- iv. 116 Red Mill Dr, Palm Coast, Florida 32164, as described in Attachment A-4 ("**REVES Residence**");

the following vehicles, which I believe to be currently located in the Middle District of Florida (collectively referred to as the "**Target Vehicles**");

- v. Silver 1998 Honda Civic bearing Florida license plate IQ13HJ, VIN: 1HGEJ8147WL075628, and driven by Billy CORDOVA, as described in Attachment A-5 ("**CORDOVA Vehicle**");
- vi. White 2020 Dodge Charger bearing Florida license plate 25BJAN, VIN: 2C3CDXHG2LH186169, and driven by Ralph MORENO, as described in Attachment A-6 ("**MORENO Vehicle**");
- vii. Black 2019 Toyota Camry bearing Florida license plate QFKG23, VIN: 4T1BZ1HK7KU026287, and driven by Justice DEL CARPIO, as described in Attachment A-7 ("**DEL CARPIO Vehicle**");

and electronically stored information concealed through technological means. This warrant authorizes the use of a remote search technique to be deployed on the computer servers hosting Telegram ("**Telegram Servers**"). Specifically, investigators may conduct this search by using any computer (as defined above) found at the **Target Residences**, in the **Target Vehicles**, or on the person of the **Target Suspects**, for which additional evidence exists that the computer was used by a **Target Suspect**,

and on which a Telegram account is located, as described in Attachment A-8.

6. The foregoing warrants are requested to search for evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 1201(c), Conspiracy to Kidnap; and 18 U.S.C. § 1201(a)(1), Kidnapping (hereinafter the “Target Offenses”). As set forth below, I have probable cause to believe that such property and items, as described in Attachments B-1 through B-8, including digital devices, electronic storage media, and cryptocurrency, are currently located at the **Target Residences**, in the **Target Vehicles**, and on the **Telegram Servers**, described below and in Attachments A-1 through A-8.

7. This affidavit is intended to show only that there is sufficient probable cause for the requested warrants and does not set forth all my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Target Offenses

8. I believe there is probable cause that evidence of the following violations will be found in the places to be searched (hereinafter the “Target Offenses”):

viii. 18 U.S.C. § 1201 provides, in part:

(a) Whoever unlawfully seizes, confines, inveigles, decoys, kidnaps, abducts, or carries away and holds for ransom or reward or otherwise any person, except in the case of a minor by the parent thereof, when—

(1) the person is willfully transported in interstate or foreign commerce, regardless of whether the person was alive when transported across a State boundary, or the offender travels in interstate or foreign commerce [. . .] in committing or in furtherance of the commission of the offense.

...

(c) If two or more persons conspire to violate this section and one or more of such persons do any overt act to effect the object of the conspiracy, each shall be punished by imprisonment for any term of years or for life.

STATEMENT OF PROBABLE CAUSE

9. I will structure the probable cause section of this affidavit as follows:

(A) Background on D.J.J. (Victim) and a summary of the Target Offenses; (B) Identification of the seven locations where the **Target Suspects** traveled during and immediately after the Target Offenses (“Suspect Locations”); (C) Identification of the **Target Suspects** and their cell phones at the time of the Target Offenses; (D-E) Training and experience concerning electronic evidence and the **Target Suspects’** use of Telegram and/or cryptocurrency; and (F-I) Each **Target Suspect’s** residence (**Target Residences**), vehicle (**Target Vehicles**), and current cell phone.

Affidavit of Jaron T. Cookson

Page 6

A. BACKGROUND ON D.J.J. AND SUMMARY OF TARGET OFFENSES***D.J.J. Wire Fraud and SIM Swapping Activity***

10. Based on my review of multiple police reports,³ an affidavit supporting the application for an FBI search warrant,⁴ conversations with other investigators, and my role in this investigation, I learned the following:

11. D.J.J. was the subject of an FBI investigation focused on wire fraud violations involving the theft of millions of dollars of cryptocurrency, District of Oregon Case Number 3:23-cr-00085-MO, which stemmed from cybercriminal activities beginning in 2019. D.J.J.'s criminal conduct is described in his plea agreement in that case and included working with others to execute SIM swapping⁵

³ Portland Police Bureau case 2023-293512 and Washington County Sheriff's Office case 2023-16923.

⁴ United States District Court for the District of Oregon Case Number 3:23-mc-984 (detailed further below).

⁵ Based on my training and experience, and conversations with other investigators, I have learned the following:

(1) A Subscriber Identity Module (hereinafter "SIM") card is a removable and separately purchasable electronic card within a cellular device that stores user data in Global System for Mobile (GSM) phones and directs wireless transmissions to specific phones. Without a SIM card, a GSM cellular phone would not be authorized to use a mobile network except to make calls to emergency services.

(2) A SIM swap scam is a fraud that occurs when a fraudster activates a new SIM card and redirects – or *ports* – the victim's telephone number to a device within the fraudster's control. Once the fraudster gains access and control over the victim's cellular phone, the fraudster(s) can then access the phone communications, in particular Short Message Service (hereinafter "SMS") text messages. The fraudster is then able to take advantage of a weakness in two-factor authentication and verification in which the second step is an SMS text message or call to the victim's cellular phone number. As such, the fraudster will receive any codes and passwords/password reset requests sent to that phone via call or text for any accounts accessible on the mobile device. After receiving the password or password reset link for an account, the fraudster will gain access to that account, change the password to lock out the legitimate user, then steal any available funds from financial applications used by the legitimate owner of those funds.

(3) Individuals will often coordinate criminal efforts with other fraudsters to effectuate a SIM swap attack and will assume specific roles within the scheme. For example, one person may find viable targets, another person may conduct social engineering attacks against a phone provider, another may develop

attacks to take over victims' online account(s) and steal cryptocurrency. I know from my review of this material that D.J.J. mostly worked with others online in various locations by communicating on online platforms such as Telegram. D.J.J. worked with co-conspirators believed to be in multiple states and even in other countries. On January 30, 2024, D.J.J. was sentenced to 72 months' imprisonment after he pleaded guilty to the foregoing criminal conduct.

12. Since 2019, D.J.J. made enemies through his online activities, including from other people engaged in the same types of criminal activity as D.J.J. Years ago, some of those enemies used other associates to travel across state lines to physically harass D.J.J. at his parents' house in Portland, Oregon.

13. Based on my training and experience, open-source research, and conversations with other investigators, I know "violence as a service" is a growing phenomenon as a form of enforcement and intimidation within the SIM swapping community. What can initially take the form of less violent harassment (*e.g.*, Doxing⁶ or Swatting⁷) can progress to physical acts of violence in order to send a message. These acts of violence often include paying individuals to travel across state lines to

malicious software to deploy against the phone providers, and others may perform money laundering activities to turn their illicit proceeds into fiat currency. Depending on the crew and specific circumstances of any given SIM swap scam, different attacker roles may be required. Individuals conspiring to commit these crimes are most often located in different states and often in different countries. They communicate over the internet and often use Telegram to communicate.

⁶ Based on open-source research, Doxing is the action or process of searching for and publishing private or identifying information about a particular individual on the internet, typically with malicious intent.

⁷ Based on open-source research, Swatting is a form of Doxing where the Doxer uses knowledge of the victim's location to make a hoax call to generate an emergency law enforcement response against a target victim.

engage in violence against someone who has either failed to uphold their part of an agreement (*e.g.*, failing to distribute the illicit proceeds), or has become uncooperative. More specifically, from my conversations with other investigators, I know that kidnappings, home invasions, firebombing, and other violent activity have all been committed by co-conspirators engaged in SIM swapping because of arguments over the handling of proceeds.

14. Based on statements made by D.J.J., as detailed below, in late October or early November 2023 (shortly before his kidnapping and assault), D.J.J. began to receive threats from at least one individual believed to be engaged in the SIM swapping community. According to D.J.J., the threats were made because D.J.J. refused to find criminal work for him.

Summary of Target Offenses: November 10, 2023, Kidnapping

15. On November 10, 2023, D.J.J. was forcibly abducted from outside of his apartment by multiple individuals that D.J.J. believed were armed with guns. Duct tape was eventually wrapped around D.J.J.'s head to serve as a blindfold, and D.J.J. was physically restrained. According to D.J.J., the people who abducted him forced him to turn over control of his email accounts and made D.J.J. read a seed phrase that gave the attackers access to D.J.J.'s cryptocurrency account(s). According to D.J.J., the attackers stole a laptop and D.J.J.'s iPhone 14, which was associated with the call number 503-481-8473 (hereinafter "D.J.J.-8473").

16. According to police reports, D.J.J.'s neighbor saw two white males wearing ski masks grab D.J.J. from the stairs in front of D.J.J.'s apartment and force him into a newer white BMW SUV (referred to hereinafter as the "Suspect BMW"). The Suspect BMW was already occupied by a driver and a passenger and did not have a rear license plate. The neighbor provided a video that he/she captured of the incident in front of D.J.J.'s apartment. See a still image from the video below:



17. According to D.J.J., he was thrown into a white SUV and driven to some unknown location until he was transferred to another vehicle, which he believed was a dark-colored van.⁸ D.J.J. could not see through the duct tape for most of the drive, but he could "hear their hand signs" to each other, such as when they were signaling to someone else in the vehicle to beat him up, or to be quiet. D.J.J.

⁸ Based on subsequent conversations with D.J.J.'s attorney, D.J.J. may have later described the van as white.
Affidavit of Jaron T. Cookson Page 10

estimated that there were at least six kidnappers, all of whom spoke Spanish, and only one of whom appeared to be fluent in English. D.J.J. was eventually taken out of the vehicle and brought to an empty field in North Plains, Oregon. D.J.J.'s feet were bound with zip ties, and he was bound with duct tape to a post in the field. His pants were left around his ankles and his underpants were still on. Hours later, a passer-by found D.J.J. still bound to the post in the field and D.J.J. asked the passer-by for help.

18. Investigators were initially told that several of D.J.J.'s fingers, his wrists, and multiple ribs were injured and possibly broken over the course of the kidnapping and assault. Investigators were also told that, according to D.J.J.'s father, D.J.J. appeared to have sustained lung damage, possibly as a result of being kicked in the chest. I have since reviewed medical records with multiple investigators and believe the assessment identified D.J.J. sustained right pneumothorax (i.e., collapsed lung), multiple fractured ribs, and multiple fractured fingers, among other ailments.

19. After D.J.J. was recovered by law enforcement, he explained that the FBI seized millions of dollars from him the year prior to his kidnapping, but he never told anyone the money was taken. D.J.J. believed his assailants thought he still had the money and kidnapped him to steal the money, which is why they were trying to gain access to his seed phrase and cryptocurrency wallets. D.J.J. eventually told his assailants he had money at his apartment, where he thought they found his recovery seeds.

20. D.J.J. provided the Portland Police Bureau (“PPB”) with consent to search his apartment. During the search, PPB located a pink hand-written note with 12 words on it, consistent with a seed phrase. On or about August 28, 2024, an FBI Portland Computer Scientist used the seed phrase to reconstitute an Exodus wallet (a cryptocurrency holding platform, or “wallet”) which showed multiple transactions of Monero (a cryptocurrency) prior to November 2023. The final transaction occurred at approximately 7:55 p.m. on November 10, 2023, when D.J.J. was allegedly mid-kidnapping. The transaction value was approximately 751.5 Monero, or approximately \$128,000 in USD (at that time) which emptied the balance.

21. Based on my training and experience, I know that Monero transactions are by design difficult to trace since Monero is an anonymity-enhanced cryptocurrency, especially when the wallet address that received the transaction is unknown, as it is with the foregoing transaction. The FBI’s attempt to identify the recipient address is ongoing, which would be helped if investigators were able to locate the recipient address (e.g., on a presently unknown digital device). However, based on the foregoing, and the investigation to date, I believe the transaction documented the theft by D.J.J.’s assailants after they located the same seed phrase.

22. D.J.J. also told investigators that approximately two weeks prior to his kidnapping, an unknown individual using the online moniker “lil James” threatened D.J.J. because D.J.J. refused to find criminal work for lil James. In response, lil James threatened to “send his MS-13 friends” after D.J.J. According to D.J.J., he

believed that lil James did not live in the United States. Based on information provided by other FBI agents with similar investigations, lil James is a known moniker of someone engaged in the SIM swapping community known to communicate and ask for work from other high profile SIM swapping actors. I know that it is common for individuals engaged in the SIM swapping community to use communication platforms like Telegram to discuss SIM swapping attacks over private or public channels, to include discussing victims and methods of attack. In addition, and as stated above, I also know that criminals within the community of which D.J.J. was a part have paid to send people across state lines to harass, intimidate, or physically assault fellow criminals in order to facilitate extortion, consistent with D.J.J.'s kidnapping.

Questions About D.J.J.'s Forthrightness and an Anonymous Tip

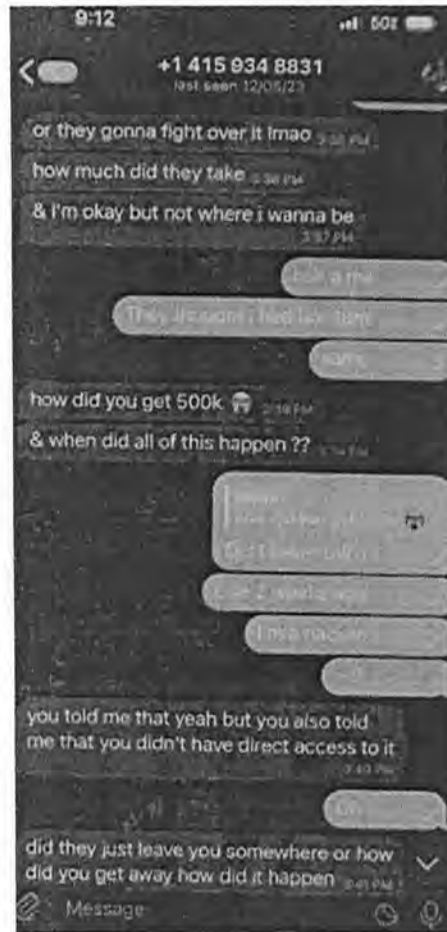
23. It should be noted that investigators do not believe D.J.J. was completely forthright in the information he provided. D.J.J., through his attorney, declined to provide a full, no questions off-limits, interview of D.J.J. immediately after the kidnapping. D.J.J. provided some information that was independently corroborated but also made seemingly conflicting statements. He also admitted to continued engagement with persons suspected of criminal conduct after pleading guilty to the foregoing charges.

24. Moreover, based on an anonymous tip, investigators believe D.J.J. continued to participate in SIM swapping activity following his change of plea to

guilty. On December 11, 2023, D.J.J. consented to a search of his Telegram account. An FBI Special Agent and I reviewed some of the chat conversations in which D.J.J. participated. We did not locate messages from D.J.J. from the time prior to his kidnapping, or with an account we knew belonged to lil James. Based on my training and experience, and conversations with the other Special Agent who reviewed these messages, this could be the result of D.J.J. changing his Telegram account between the time of his kidnapping and the time of our consent search.

25. In general, the messages we did review (specifically the ones after his kidnapping) showed D.J.J. was involved in criminal activity by obtaining and possessing social security numbers, dates of birth, and other Personal Identification Information of individuals that he was most likely targeting as part of his criminal activity. The government filed a motion to revoke D.J.J.'s pretrial release given the evidence of his ongoing criminal activities, and the court did revoke his release prior to sentencing given his continued criminal conduct.

26. However, some of the Telegram messages were also consistent with his statements to investigators. For example, in one conversation, D.J.J. explained that the kidnappers took money from him (D.J.J.'s conversation is on right-hand side of capture):



27. Based on my training and experience, I believe “half a mil” is slang for half of one million dollars. I believe “10m” is shorthand for ten million dollars, and that D.J.J. thought his kidnappers believed he had that much money. In a later conversation, D.J.J. realized that the kidnappers did not steal all of the “half a mil” he claimed to have, noting that they only stole “200k.”



28. Given that D.J.J. had no known legitimate source of income, as well as the other indicators that D.J.J. was engaged in fraud, I believe all of the cryptocurrency possessed by D.J.J. were the proceeds of criminal activity.

B. IDENTIFICATION OF THE SEVEN SUSPECT LOCATIONS

29. On November 14, 2023, the Honorable Jeffrey Armistead, United States Magistrate Judge, District of Oregon, signed a search warrant (3:23-mc-984) authorizing the collection of historic and prospective geolocation data from D.J.J.-8473.⁹ Based on my review of the geolocation data, I believe D.J.J.-8473 was left on for over 12 hours following D.J.J.'s kidnapping. An FBI Special Agent on the

⁹ Investigators corroborated that D.J.J.-8473 belonged to D.J.J. via open-source research and D.J.J.'s own statements to law enforcement.

Cellular Analysis Survey Team (“CAST”) and I reviewed the geolocation information from the time of D.J.J.’s kidnapping, until D.J.J.-8473 stopped generating location information. Based on this review, we identified seven locations where we believe D.J.J.-8473 traveled during and immediately following D.J.J.’s kidnapping (“Suspect Locations”). In addition, I reviewed video surveillance at businesses in the vicinity of multiple Suspect Locations at times consistent with when D.J.J.-8473 indicated the phone should be in the vicinity of that Suspect Location. See an approximate representation of the seven Suspect Location in the image below:



30. Detailed below are observations supporting my belief that D.J.J.-8473 was located at each of the Suspect Locations at or around the times¹⁰ designated:

¹⁰ The times identified below are all in Pacific Time and are based on the times displayed by the video

Location 1: Portland, Oregon, Near D.J.J.'s Apartment

31. D.J.J. was reportedly kidnapped from the area in front of his apartment, on SW 11th Ave. between SW Market St. and SW Clay St., Portland, Oregon, near the coordinates 45.514615, -122.686391 ("**Location 1**"). I reviewed video surveillance at the 11 Marche' Apartments, 1115 SW Market St., Portland, Oregon, which captured the vicinity of **Location 1**. The video quality and lighting were poor, but based on my review, between approximately 5:20 p.m. and 5:22 p.m.,¹¹ the silhouettes of multiple people appeared to approach the area in front of D.J.J.'s apartment building. Around the same time, a white SUV pulled in front of the apartment building, facing the wrong way on a one-way street. The silhouettes of at least two individuals then moved quickly from the front of the apartment building toward the white SUV, in a manner I believe was consistent with forcing one of the individuals into the back seat¹². I later determined the SUV was a white 2011 BMW X5,¹³ referred to hereinafter as the "Suspect BMW." Geolocation information for D.J.J.-8473 was consistent with the device being near the vicinity of **Location 1** prior to the kidnapping and then moving as though in a vehicle around 5:18 p.m. D.J.J.-

surveillance and/or geolocation information. All times should be interpreted as estimates.

¹¹ Based on police reports, D.J.J. estimated he was kidnapped around 7:00 p.m., on his walk back from a nearby convenience store, later identified as the Plaid Pantry. Based on my review of video surveillance from the Plaid Pantry, D.J.J. exited the Plaid Pantry between approximately 5:17 p.m. and 5:22 p.m.

¹² Previous affidavits stated multiple people appeared to pull someone from the area in front of D.J.J.'s apartment building and pushed the individual into the back of a white SUV. This explanation was modified herein to be a more precise detailing of my observations.

¹³ D.J.J. described the SUV as a white Toyota. At least one witness described it as a white BMW.

8473 appeared to return later to the vicinity of **Location 1** and was consistent with being there at multiple points between 5:18 p.m. and 10:05 p.m.

Location 2: North Plains, Oregon, Near The Field Where D.J.J. Was Recovered

32. D.J.J. was recovered from a field west of NW Mountindale Rd. and NW Old Pumpkin Ridge Rd., North Plains, Oregon, less than 600 meters west of the coordinates 45.606767, -123.013454 ("**Location 2**"). Investigators were not able to locate video surveillance capturing the vicinity of **Location 2**. Geolocation information for D.J.J.-8473 indicated it was near or in the vicinity of **Location 2** for multiple periods between 10:45 p.m. on November 10, 2023, and 1:35 a.m. the next morning (November 11, 2023). I believe the more precise location information generated by D.J.J.-8473 was consistent with frequently placing D.J.J.-8473 between one and three miles northwest and west of **Location 2**. From 12:44 a.m. to 1:34 a.m., less precise location information was consistent with placing D.J.J.-8473 in the vicinity of **Location 2**.

Location 3: Hillsboro, Oregon, After D.J.J. Was Abandoned

33. At approximately 1:55 a.m., D.J.J.-8473 appeared to stop near the intersection of Highway 26 and NW 185th Ave., Hillsboro, Oregon for over 15 minutes. Investigators were unable to locate the suspect vehicles on video surveillance but believe the stop was consistent with briefly exiting the highway near the coordinates 45.53831, -122.86623 ("**Location 3**").

Location 4: NW Lower River Rd., Vancouver Lake, Washington

34. Geolocation information for D.J.J.-8473 appeared consistent with the phone traveling along the west side of Lake Vancouver and back, using NW Lower River Rd., between approximately 3:17 a.m. and 3:35 a.m. (“**Location 4**”¹⁴). I subsequently reviewed video surveillance maintained by the Port of Vancouver USA, 3103 NW Lower River Road, Vancouver, Washington (“Port Video”). The camera captured the area west of W Fourth Plain Blvd and St Francis Ln¹⁵, Vancouver, Washington, which was the primary access road to **Location 4**. Based on my review of the Port Video, at approximately 3:19 a.m. a white SUV consistent with the Suspect BMW entered the view of the camera, traveling west toward the vicinity of **Location 4**. Approximately 13 minutes later, what appeared to be the same vehicle reentered the view of the camera traveling east, away from **Location 4**. Both times were consistent with geolocation information generated by D.J.J.-8473.

Location 5: Felida Store Mini Mart, Vancouver, Washington

35. Geolocation information for D.J.J.-8473 indicated the phone traveled to the vicinity of 45.712493, -122.708377 (“**Location 5**”) between 3:37 a.m. and 3:45 a.m. These coordinates were in the vicinity of the Felida Store Mini Mart, 12604

¹⁴ **Location 4** is more specifically based on the coordinates 45.669257, -122.743809, which investigators subsequently used to obtain cellular tower location information, as detailed herein.

¹⁵ Previous affidavits described the area captured by the camera as “the area west of W Fourth Plain Blvd and W 26th Ave.” The image in those affidavits similarly reflected this area. Investigators have since determined the intersection of W Fourth Plain Blvd and St Francis Ln is more accurate, which will be reflected in affidavits going forward.

NW 36th Ave., Vancouver, Washington ("Felida Store"). I reviewed video surveillance at the Felida Store which captured the parking lot and gas pump in front of the store. Based on my review, at approximately 3:39 a.m., a white SUV, consistent with the Suspect BMW, entered the parking lot and parked in front of a gas pump. An adult male exited the vehicle, walked toward the store, returned to the vehicle, and departed before 3:43 a.m.

Location 6: Speedway Mini Mart, Vancouver, Washington

36. Geolocation information for D.J.J.-8473 indicated the phone traveled eastbound through the vicinity of 45.721878, -122.661585 around 3:45 a.m. ("Location 6"). I reviewed still images taken from video surveillance maintained by a Speedway Mini Mart, 14300 NE 20th Ave., Vancouver, Washington ("Speedway"), less than 900 meters northeast of Location 6. The still images captured the interior of the Speedway and its exterior gas pumps. The investigator who initially reviewed the video and provided me with the still images confirmed a white SUV consistent with the Suspect BMW arrived at approximately 3:53 a.m.¹⁶ Shortly after, an adult male, consistent with the adult male observed at the Felida Store, entered the Speedway. Within a few minutes the adult male exited the Speedway and the Suspect BMW departed shortly thereafter.

¹⁶ The investigator who reviewed the video confirmed the video's displayed time was approximately 30 minutes slow. I believe this accounts for the discrepancy in the camera's displayed time and the time the investigator reported the Suspect BMW departed.

Location 7: Airbnb, 2208 E 25th St, Vancouver, Washington

37. Geolocation information for D.J.J.-8473 indicated the phone later traveled to the vicinity of 45.638502, -122.648089 ("**Location 7**"), which was near the parking lot north of Burgerville, 2200 E 4th Plain Blvd., Vancouver, Washington ("Burgerville"). The phone appeared to be stationary for large periods between 4:31 a.m. and 8:57 a.m. I reviewed video surveillance maintained by the McDonald's at 2110 E 4th Plain Blvd, Vancouver, Washington ("McDonald's"). The McDonald's camera captured the parking lot immediately north of Burgerville and an Airbnb rental that, as detailed below, I believe was frequented by the **Target Suspects**. The Airbnb address was 2208 E 25th St., Vancouver, Washington ("Airbnb"). See the image below which shows **Location 7** in relation to the McDonald's, Burgerville, and Airbnb:



38. Based on my review of the McDonald's video, I observed a white SUV consistent with the Suspect BMW come and go from the Burgerville parking lot over multiple hours consistent with the arrival and departure of D.J.J.-8473. For example, a vehicle consistent with the Suspect BMW arrived at approximately 4:31 a.m. and departed at 5:47 a.m., consistent with D.J.J.-8473's arrival and departure. Later, at approximately 8:51 a.m., while the Suspect BMW was in the Burgerville parking lot, a dark minivan consistent with a Toyota Sienna ("Suspect Toyota"), backed out of the driveway associated with the Airbnb, entered the Burgerville parking lot, and parked in front of the Suspect BMW. The position of the two Suspect Vehicles was

consistent with a meeting between the vehicles' occupants. Both vehicles departed around 8:56 a.m., consistent with the departure of D.J.J.-8473. See images of the Suspect Toyota pulling out of the Airbnb and parking in front of the Suspect BMW below:



39. On multiple occasions the McDonald's video captured one or more persons walking from the Suspect BMW toward the Airbnb, or vice versa, in a manner consistent with the Suspect BMW's occupants entering or exiting the Airbnb. As detailed below, I believe the occupants of the Airbnb were co-conspirators in the Target Offenses.

40. In addition to the above time periods, the McDonald's video also captured the Suspect BMW and the Suspect Toyota enter the area captured by the camera at approximately 2:40 a.m. on November 11, 2023. The Suspect Toyota parked in the Airbnb driveway and the Suspect BMW parked in the Burgerville parking lot. At least two occupants of the Suspect BMW exited the vehicle and walked toward the Airbnb, consistent with entering it. The Suspect BMW did not depart until 2:56 a.m., after two individuals walked from the vicinity of the Airbnb, entered the Suspect BMW, and departed (consistent with the Airbnb video

timestamp detailed below). D.J.J.-8473 did not generate location information between 2:30 a.m. and 3:01 a.m. to corroborate these observations, but **Location 7** was consistent with the direction to which D.J.J.-8473 was traveling prior to 2:30 a.m. In addition, the location of D.J.J.-8473's at 3:01 a.m. was consistent with the Suspect BMW departing at 2:56 a.m. Based on the foregoing, I believe the Airbnb was where both Suspect Vehicles traveled following the kidnapping.

C. IDENTIFICATION OF TARGET SUSPECTS AND CELL PHONES

Billy CORDOVA (Suspect 1) and CORDOVA-1128

41. According to Airbnb's records, the aforementioned Airbnb was reserved by Billy CORDOVA ("CORDOVA") from November 8 to 12, 2023. However, the manager of the Airbnb rental reportedly received a message on November 11, 2023, indicating CORDOVA checked out on November 11, 2023 (the morning after the kidnapping). CORDOVA's listed phone number and email address were 904-674-1128 ("CORDOVA-1128") and billycordova720@gmail.com ("CORDOVA's Email").

42. I queried CORDOVA-1128 in a subscription-based open-source database and determined the number was associated with "Billy CORDOVA." I also reviewed records obtained from AT&T on or about May 13, 2024, which listed Alma Hamitaj ("Hamitaj") as the name for CORDOVA-1128's Financial Liabile and Billing Party, but CORDOVA was the listed User of CORDOVA-1128, which was activated on March 12, 2022, and was listed at that time as Active.

43. On January 23, 2024, the Honorable Stacie F. Beckerman, United States Magistrate Judge, District of Oregon, signed warrants authorizing the collection of location information from CORDOVA-1128 (3:24-mc-73) and from AT&T cell towers servicing the Suspect Locations (3:24-mc-70). I compared the location information generated by CORDOVA-1128 to that generated by D.J.J.-8473 and believe both devices appeared to regularly be in the same vicinity while traveling between Suspect Location 1 and Suspect Location 7 at times consistent with the activities detailed above. For example, I believe CORDOVA-1128 was in the area near Location 1 shortly before D.J.J. was kidnapped. Between 10:20 p.m. and 10:50 p.m., both CORDOVA-1128 and D.J.J.-8473 travelled west toward Location 2 and appeared to regularly be in the same vicinity along the way. CORDOVA-1128 and D.J.J.-8473 then traveled east from Location 2 toward Location 3 around 1:37 a.m. on November 11, 2023. Both devices appeared to travel away from Location 2, even though at the time, I believe D.J.J. was bound to a post at Location 2. CORDOVA-1128 and D.J.J.-8473 appeared to then travel to the remaining locations (Locations 4-7) at similar times and appeared to regularly be in the same or nearby area. In addition, the Suspect BMW was also observed in multiple locations at times similar to CORDOVA-1128 and D.J.J.-8473. Based on the foregoing, I believe the travel patterns of both devices were at times consistent with traveling in the same or nearby vehicles for large portions of the location data; though there were smaller periods

(e.g., later in the morning on November 11, 2023) when the devices appeared to separate.

44. I also believe the location information generated by CORDOVA-1128 was consistent with departing Orlando International Airport, Orlando, Florida (“MCO”) on November 8, 2023, and landing at Portland International Airport (“PDX”) the same day. CORDOVA-1128 then appeared to depart PDX on November 11, 2023, and arrived at MCO on November 12, 2023.

45. According to Delta Airline records, CORDOVA was one of three passengers on the same roundtrip flight reservation between MCO and PDX, departing November 8, 2023, and scheduled to return November 12, 2023. The two additional passengers were Ralph MORENO (“MORENO”) and Justice DEL CARPIO (“DEL CARPIO”). Jackson REVES (“REVES”) was also a listed passenger on the same flights, using the same credit card number and phone number for the reservation, but it appeared to be purchased separately. Delta airline’s records indicated the four passengers (i.e., **Target Suspects**) did not board their original November 12, 2023, return flight from PDX to MCO, but instead purchased a new return flight on November 11, 2023, which listed all four passengers (i.e., **Target Suspects**) on the same reservation.

Location Information and Search History from CORDOVA’s Email

46. On July 8, 2024, Judge Beckerman signed a warrant (3:24-mc-709 A) authorizing the collection of content from the Google account

billycordova720@gmail.com ("CORDOVA's Email"). The affidavit supporting that application established probable cause that CORDOVA was the user of the email. I reviewed Google's records and found that on November 8, 2023, between approximately 4:00 p.m. and 5:00 p.m., CORDOVA searched the address of the Airbnb, the apartment complex in which D.J.J. resided, and Mountindale, Oregon (less than 2 miles northwest of the location from where D.J.J. was recovered on November 11, 2023). The account also made multiple Portland-area searches prior to November 8, 2023 (when the **Target Suspects** arrived in Oregon).

47. Based on the foregoing, and the investigation to date, I believe CORDOVA participated in the Target Offenses and used CORDOVA-1128 at the time the Target Offenses were committed.

Ralph MORENO (Suspect 2), Suspect BMW, and MORENO-5756

48. During the review of the Felida Store video (Location 5), I observed what appeared to be an Oregon license plate on the Suspect BMW. The license plate appeared to include the middle characters "93NZ," but the first and last character were not clearly decipherable. I subsequently reviewed vehicles advertised for rent on the car sharing marketplace known as Turo, Inc. ("Turo"), and discovered an advertisement for a 2011 BMW X5 bearing Oregon license plate "793NZF." I compared the make, model, and license plate of the vehicle and believe the vehicle was the same vehicle captured by the Felida Store video. I also believe it was the same vehicle captured by D.J.J.'s neighbor outside of D.J.J.'s apartment, despite the

vehicle in that video not having a rear license plate. Based on my training and experience I believe persons planning to engage in criminal conduct may remove their license plate to avoid detection by law enforcement. See images of the vehicle from the Felida Store video and Turo advertisement below:

Felida Store Mini Mart, 12604 NW 36th Ave., Vancouver, Washington



Turo Advertisement



49. According to Turo records, the Suspect BMW was booked by Ralph MORENO (“MORENO”) on November 7, 2023. The reservation was from November 8, 2023, to November 12, 2023. MORENO's listed phone number was 386-346-5756 (“MORENO-5756”). I contacted the Suspect BMW's listed “Host” who showed he/she received a message from MORENO-5756 on November 11, 2023, saying MORENO-5756 had a family emergency and had returned the vehicle that day. See an additional image of the Suspect BMW provided by Turo below:



50. An FBI Portland Analyst queried MORENO-5756 in a subscription-based open-source database and determined the number was associated with MORENO. On or about June 3, 2024, Verizon's records listed Ralph S MORENO as MORENO-5756's subscriber, with a listed Effective Date of October 11, 2022, and a Disconnect Date of March 29, 2024.

51. On January 23, 2024, Judge Beckerman signed warrants authorizing the collection of location information from MORENO-5756 (3:24-mc-74) and from Verizon cell towers servicing the Suspect Locations (3:24-mc-72). The historic location information associated with MORENO-5756 was limited and was not precise but it appeared consistent with MORENO-5756 traveling from Florida to Oregon on November 8, 2023, and returning to Florida on November 12, 2023, consistent with the flight reservations mentioned above. The last reliable historic

location information that Verizon provided for MORENO-5756 on November 10, 2023, was at approximately 3:05 p.m. and 3:20 p.m. At that time, MORENO-5756 was in the same area as CORDOVA-1128. The next reliable location was on November 11, 2023, at approximately 9:28 a.m., at which time it appeared to be in Portland, Oregon in the same area as CORDOVA-1128.

52. An FBI Special Agent on CAST and I reviewed the data from Verizon cell towers servicing the Suspect Locations and did not locate MORENO-5756 in the cell tower data. Based on my training and experience, and conversations with other investigators, I know the Verizon cell towers would not have location information for MORENO-5756 if it was off during the Target Offenses, which I believe is consistent with the lack of historic location information during that same period. In addition, MORENO-5756's toll records showed multiple calls made to MORENO-5756 at 12:39 a.m., each of which went directly to voicemail, and MORENO-5756 had no cell site at the time of the calls, which was consistent with the phone being off.

53. Based on the foregoing, and the investigation to date, I believe MORENO participated in the Target Offenses and used MORENO-5756 at that time.

Justice DEL CARPIO (Suspect 3), DEL CARPIO-0534, and Suspect Toyota

54. As mentioned above, Delta's records showed the Target Suspects had round-trip flights between MCO and PDX, but they did not board their scheduled

November 12, 2023, return flight. Instead, they made a new Delta reservation that included all four passengers on the same reservation, departing PDX and laying over at Los Angeles International Airport ("LAX"). According to Delta's records, they did not board their connection flight after arriving at LAX. Instead, according to Spirit Airline's ("Spirit") records, they made a Spirit reservation for the same four passengers departing LAX and eventually landing at MCO on November 12, 2023. According to Spirit records, DEL CARPIO's listed phone number for the flight reservation was 386-515-0534 (DEL CARPIO-0534).

55. According to Turo records, DEL CARPIO reserved a Toyota Sienna from November 8 to November 12, 2023. I believe the make, model, and color of the vehicle were consistent with the Suspect Toyota identified at Location 7. I will refer to both as the Suspect Toyota hereinafter. DEL CARPIO-0534 was the listed phone number on the Turo reservation, and 50 Cooper Ln, Palm Coast, FL was the listed address. DEL CARPIO-0534 was used to exchange multiple messages with the Turo Host, including a message on November 11, 2023, telling the host he was flying home that day due to an emergency, and he would therefore return the vehicle that day. See an image of the Suspect Toyota captured by the McDonald's video surveillance compared to an image from Turo below:



56. As stated above, Turo provided records for both DEL CARPIO's reservation of the Suspect Toyota and MORENO's reservation of the Suspect BMW. One of the images I found in DEL CARPIO's records was a picture of himself holding a driver's license. One of the images I found in MORENO's records included the Suspect BMW, with an individual that I believe is consistent with DEL CARPIO standing next it. I also believe the Suspect Toyota can be seen in the background of that image with the side door open. See below for the image of DEL CARPIO from DEL CARPIO's Turo records, compared to the image of DEL CARPIO and both Suspect Vehicles, found in MORENO's Turo records:



57. Investigators also obtained video surveillance from the aforementioned Airbnb for the period the suspect BMW frequented it. The Airbnb video was limited but captured at least four individuals entering and/or exiting the Airbnb between November 9 and 11, 2023. One of the individuals appeared consistent with DEL CARPIO. See below for an image taken from the Airbnb video compared to the Turo images:



58. On or about June 3, 2024, Verizon's records listed Jahzi See Del Carpio as DEL CARPIO-0534's subscriber, which was listed as Active since November 10, 2020. The listed address was 6 Flemington Ln, Palm Coast, Florida ("**DEL CARPIO Residence**"). I know Jahzi Del Carpio ("Jahzi") was the listed payment name on at least one of the Delta flight reservations mentioned above. I also believe he is the older brother of DEL CARPIO (Suspect 3). Based on Verizon records between October 1, 2023, and February 22, 2024, I believe Jahzi was the listed subscriber for multiple phones during that period, to include the phone used by DEL CARPIO (DEL CARPIO-0534). I queried a subscription-based open-source database using the address listed on the Verizon account (**DEL CARPIO Residence**) and saw it was associated with DEL CARPIO, Jahzi Del Carpio, and Savior Del Carpio, all three of whom were recently also associated with 50 Cooper Ln, Palm Coast, Florida (the address listed in DEL CARPIO's Turo reservation). An FBI Special Agent on CAST and I reviewed the data from Verizon cell towers servicing the Suspect Locations and did not locate DEL CARPIO-0534 in the cell tower data.

59. On June 7, 2024, the Honorable Jolie A. Russo, United States Magistrate Judge, District of Oregon, signed a warrant authorizing the collection of historic and prospective location information from DEL CARPIO-0534 (3:24-mc-623 C). The historic location information around the time of the Target Offenses was

limited and was not precise. However, it was consistent with DEL CARPIO-0534 traveling from Florida to Oregon on November 8, 2023, and arriving in Florida again on November 12, 2023, consistent with the flight reservations mentioned above.

60. Based on the foregoing, and the investigation to date, I believe DEL CARPIO participated in the Target Offenses and used DEL CARPIO-0534.

Jackson REVES (Suspect 4) and REVES' Cell Phone

61. As stated above, Delta and Spirit's records showed REVES travelled roundtrip between MCO and PDX with the other Target Suspects. Based on a subscription-based open-source database, REVES was associated with the phone number 386-569-5791 ("**REVES Cell Phone**"). According to records I reviewed from T-Mobile on or about February 22, 2024, Ozlem REVES ("Ozlem") was the listed subscriber for the **REVES Cell Phone** from April 19, 2019, until REVES became the listed subscriber beginning December 7, 2023 (less than one month after the Target Offenses). The listed address for both Ozlem and REVES was 116 Red Mill Dr, Palm Coast, Florida ("**REVES Residence**"). On or about May 9, 2024, T-Mobile records still showed REVES as the listed subscriber for **REVES Cell Phone**, which was still listed as Active. Based on the foregoing, I believe REVES was the user of the **REVES Cell Phone** at the time of the Target Offenses, even though Ozlem was the listed subscriber. T-Mobile also provided the IMEI and IMSI numbers associated with the **REVES Cell Phone**.

62. On January 23, 2024, Judge Beckerman signed a warrant authorizing the collection of location information from T-Mobile cell towers servicing the Target Locations around the time of the Target Offenses (3:24-mc-71). An FBI Special Agent on CAST and I located the IMEI and IMSI associated with the **REVES Cell Phone** in the T-Mobile cell tower data for towers servicing Suspect Locations 1-4 and 6-7. Based on the cell tower data, I believe the times **REVES Cell Phone** was in the vicinity of these Suspect Locations were consistent with **REVES Cell Phone** traveling with CORDOVA-1128 and D.J.J.-8473, including traveling from the location where D.J.J. was kidnapped to the area where D.J.J. was later recovered. Based on these observations, and those detailed below, I believe the operator of the **REVES Cell Phone** (i.e., REVES) was involved in the Target Offenses.

63. In addition, I reviewed a DMV image of REVES and believe it was consistent with the adult male captured by the video collected from the Felida Store ("Location 5"), the still images obtained from the Speedway Mini Mart ("Location 6"), and the Airbnb video. See images of each below:

DMV Photo



Felida Store (11/11)



Speedway Mini Mart (11/11)



Airbnb (11/10)



Airbnb (11/11 at 2:55 a.m.)



64. On June 7, 2024, Judge Russo signed a warrant authorizing the collection of historic and prospective location information from the **REVES Cell Phone** (3:24-mc-623 E). This additional historic location information from around

the time of the Target Offenses was limited and was not precise. However, it did appear consistent with the **REVES Cell Phone** traveling from Florida to Oregon on November 8, 2023, and arriving again in Florida on November 12, 2023, consistent with the flight reservations mentioned above.

65. Based on the foregoing, and the investigation to date, I believe REVES participated in the Target Offenses and used the **REVES Cell Phone**.

66. As stated above, on September 10, 2024, a grand jury indicted the **Target Suspects** for the Target Offenses, and the **Target Suspects** are currently subject to arrest warrants.

Association of the Target Suspects Before and After the Target Offenses

67. On July 8, 2024, Judge Beckerman signed multiple warrants¹⁷ authorizing the collection of two Google accounts (CORDOVA's and MORENO's), three iCloud accounts (MORENO's, DEL CARPIO's, and REVES'), and three Instagram accounts (MORENO's, DEL CARPIO's, and REVES'). The affidavit supporting the application for each of those warrants established probable cause that they were the accounts' respective users, which was further corroborated by my ongoing review of the responsive records.

68. Based on my review of those accounts and toll records from each of their cell phones, I believe each **Target Suspect** had contact with at least one other **Target Suspect** leading up to the Target Offenses. I also know they shared the

¹⁷ 3:24-mc-709 A-B; 3:24-mc-710 A-C; 3:24-mc-711 A-C.
Affidavit of Jaron T. Cookson

foregoing flight reservations and appeared to have varying degrees of continued communication following the Target Offenses.. In addition, an FBI Portland Analyst provided me with an image he found on a publicly accessible Facebook account. The Facebook post was dated January 6, 2024, and included CORDOVA, MORENO, DEL CARPIO, REVES, Jordan Munoz (identified below as an associate of the **Target Suspects**), and Jahzi Del Carpio. See the image below:



D. TRAINING AND EXPERIENCE: ELECTRONIC EVIDENCE

69. Based on the foregoing, I believe the **Target Suspects** conspired together to commit the Target Offenses. I also believe evidence of their knowledge, intent, and participation in the Target Offenses will be located on the computers (including cell phones) and electronic storage mediums specifically used by the **Target Suspects**, particularly those capable of storing encrypted communications (*e.g.*, Telegram), cryptocurrency (*e.g.*, cryptocurrency addresses that received the Affidavit of Jaron T. Cookson

Page 40

alleged theft from D.J.J.), and/or other digital evidence of the Target Offenses (e.g. stored media, QR codes linked to cryptocurrency wallets, seed phrases, etc.). I will refer to these devices collectively as the **Target Devices**. I know the **Target Devices** can also be linked to or used to access various accounts associated with the Target Offenses (e.g., phone numbers, email accounts, social media accounts, etc.). As such, I believe finding the **Target Suspects** in possession of a **Target Device** with the foregoing stored communications, cryptocurrency, media, or relevant accounts constitutes evidence of the **Target Suspects'** knowledge and involvement in the Target Offenses.

70. Moreover, based on my training, experience, and knowledge of this investigation, I know that digital devices and computer files and remnants of such computer files can be recovered months or even years after being used. In addition, in my training and experience, it is common for individuals to back up or preserve copies of digital media across multiple devices to prevent loss. Indeed, some companies provide services that seamlessly sync data across devices, such as Apple devices and the Apple iCloud service. Thus, there is reason to believe that evidence of the Target Offenses may be saved on multiple **Target Devices** specifically used by the **Target Suspects**.

71. I also know from my training and experience that even when criminal actors "wipe" their computers to avoid leaving incriminating evidence, they often maintain evidence of criminal activity on removable storage media such as portable

hard drives, optical disks, and USB “thumb” drives. Additionally, cryptocurrency is sometimes stored in “hardware wallets” which are separate storage devices resembling USB drives, and the recovery keys to their wallets are sometimes written down on paper, allowing investigators to identify proceeds from criminal activity which resulted in obtaining cryptocurrency (e.g., the alleged theft of cryptocurrency from D.J.J.).

72. For clarity, I will provide a brief summary of my training and experience regarding two types of electronic evidence that I believe are particularly relevant to this investigation: Telegram (and other encrypted communication platforms) and cryptocurrency.

Telegram and Encrypted Communication Platforms

73. Based on my training and experience, I know that crimes carried out by more than one person often involve some amount of communication among those involved. I know from training and experience that electronic devices capable of sending and receiving calls and messages (e.g., cell phones and computers) are often used for this purpose and that a cell phone or computer recovered from a participant in such criminal activity often contains evidence of communications among accomplices.

74. I have learned that Telegram (also known as “Telegram Messenger”) is a mobile and desktop messaging application used to exchange messages and media between users. Two of the features offered by Telegram are “Groups” which are chat

rooms accessible by invitation only, and "Secret Chats," which uses end-to-end encryption that allows only the sender and recipient to view the content of the chats. These secret chats can also disappear and can be set to self-destruct. Thus, it is difficult for law enforcement to gain access to these communications without access to the actual device(s) used to send or receive them.

75. I know from my training and experience that Telegram has historically refused to respond to legal process from the United States, making it difficult to obtain without gaining access to the account, often through the physical device linked to that account by the phone number. It is therefore common, based on my training and experience, for individuals engaged in criminal activity to discuss their activity over Telegram. Based on my conversations with an investigator familiar with the SIM swapping community (including D.J.J.'s personal criminal history), I know that Telegram is a primary communication platform used by SIM swappers to discuss their criminal activities. I also know that various public and private channels on Telegram are devoted to discussions about SIM swapping attacks where individuals discuss potential and actual victims, as well as methods for carrying out such attacks.

76. I believe these communications will also assist law enforcement with furthering this investigation to include helping identify additional, unknown suspect(s) involved (if applicable) and their motive in carrying out the Target Offenses.

Cloud Storage and the Transfer of Content Between Devices

77. As stated above I know certain cloud-based storage services allow a user to sync data across digital devices. I also know certain cloud services enable a user to transfer data from one digital device to a newly acquired digital device. For example, based on my training and experience, if a Telegram user logs into his or her Telegram account from a new device, while maintaining control over the phone number linked to that Telegram account, Telegram can load the user's historic activity from their **Telegram Servers**, including chats, messages in groups, etc. I also know a Telegram user can link their account to a new phone number, if they maintain control over both the previously linked phone number and their new number, allowing them to access their historic Telegram activity from their new device and/or number.

78. I know from my training and experience that specific monikers, or "handles," are associated with reputations that may be valuable in online communities. While people who participate in the previously described criminal activity are known to change phone numbers frequently for security reasons, they may want to maintain their handles for ease of recognition online. For that reason, I believe it is common for Telegram users desiring to grow or maintain a reputable handle to associate their new phone numbers (when applicable) with their same handle, making their chats potentially retrievable despite the change in device and/or number (e.g., those chats that occurred at the time of the Target Offenses).

Background on Cryptocurrency

79. Based on my training and experience, and conversations with other investigators experienced with cryptocurrency, I know cryptocurrency is a decentralized, peer-to-peer, network-based medium of value exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Cryptocurrency can exist digitally on the internet, in an electronic storage device, or in cloud-based servers. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.

80. Based on my knowledge and experience with criminal investigations involving cryptocurrency, conversations with other investigators familiar with the same, I know certain cryptocurrency wallets can only be accessed or recovered using a seed phrase, which is typically a sequence of 12 or 24 words, and users are frequently encouraged to record them in writing for safekeeping. These records often include details for transactions used to convert digital/cryptocurrency to fiat money, including through the use of online platforms that transfer funds to traditional bank

accounts or other services that provide cash delivered to a physical address in exchange for digital/cryptocurrency. Successfully tracing the origin of cryptocurrency payments often depends on the proximity of those payments to an originating exchange service. Several large exchange services collect customer data including email addresses, phone numbers, and identification documents that can be used to associate cryptocurrency addresses with their owners. A user could alternatively avoid linking their funds to an exchange and retain anonymity.

81. Based on my training and experience, I know that converting cryptocurrencies across different blockchains, also known as “chain-hopping,” makes tracing the funds more difficult for law enforcement and is a common money laundering tactic employed by cybercriminals. From my training and experience, and conversations with other investigators, I know that Monero (the cryptocurrency that I believe the **Target Suspects** took from D.J.J.) is a cryptocurrency that is by design difficult to trace and is therefore often used as the preferred cryptocurrency to disguise or launder assets. I know Monero can then be converted to other cryptocurrencies like Bitcoin (“BTC”) for eventual conversion to the U.S. Dollar equivalent. As a result, locating as many cryptocurrency addresses used by the **Target Suspects** will assist law enforcement with determining the recipients of the illicit proceeds.

82. Based on my training and experience, and conversations with other investigators, I know that individuals involved in theft of cryptocurrency and other

fraudulent or criminal activity often maintain records (including financial records, receipts, notes, ledgers, mail, tax records, and other papers) related to their crimes, and that these records are often maintained at places where the individuals can have ready access to them, including their residence. In my training and experience, I also know that individuals who have committed crimes using computers (as defined above), such as I believe the **Target Suspects** did, often keep records of their crimes in digital or electronic format, such as on a computer, and that computers are often stored in a residence.

83. It should be noted that because the **Target Suspects'** crimes involved the use of cryptocurrency, the items to be seized could be stored almost anywhere within a residence, in both physical and electronic formats. For example, Attachments B-1 through B-8 seek cryptocurrency addresses, private keys, root keys, PGP keys, and passwords. These pieces of data comprise long and complex character strings, and in my training and experience I know that many cryptocurrency users write down or otherwise record and store such items because they are too long to commit to memory. As such, these keys, passwords, and addresses may be documented in writing and secreted anywhere within a residence. For all of the foregoing reasons, I respectfully submit that probable cause exists to believe that such records, data, and documents will be found within the **Target Residences** and/or **Target Vehicles**, including in computers or on other devices that store electronic data.

E. TARGET SUSPECTS: TELEGRAM AND/OR CRYPTOCURRENCY

84. As stated above, due to Telegram's infrastructure, security, and the inability to effectively serve legal process to collect subscriber or customer information, it is difficult to identify an individual's specific Telegram account or prove their use of Telegram. I know D.J.J. previously used multiple internet-based communication platforms, including Telegram, to communicate with others engaged in criminal activity like SIM swapping. I observed some of these communications while reviewing D.J.J.'s Telegram account, as detailed above. I also know from speaking with other agents involved in these types of investigations that individuals involved in SIM swapping often discuss their criminal activities, including "violence as a service," on Telegram.

85. I know from my training and experience that SIM swapping relies on taking over control of someone else's phone number, which gets re-routed to a phone/SIM card controlled by a "holder." Holders are often responsible for the purchase of bulk quantities of SIM cards and may control several phone numbers at one time. This expertise, which is essential to successful SIM swaps, also enables SIM swappers to establish accounts (such as on encrypted messaging platforms) using valid phone numbers that law enforcement does not have a record of ever having been associated with that suspect.

86. In addition to this training and experience, and conversations with other investigators, I observed what I believe were multiple references to Telegram in

three of the four **Target Suspects'** iCloud and/or Instagram accounts. These observations are detailed below, along with my observations of each suspect's use of cryptocurrency.

MORENO's Use of Telegram and Cryptocurrency

87. While reviewing MORENO's Instagram account (username "drugcoast" and Target¹⁸ 418652453), I observed a conversation between MORENO and the Instagram user "getyabredupk" (Target 6641269800). On or around November 27, 2023, MORENO asked "Got tele ?" The user getyabredupk responded "Ofc tr3y8383[.]" Based on my training and experience (and the recorded conversation with REVES, detailed below), I know "tele" is a common abbreviation for Telegram. I believe MORENO was asking this Instagram user if he or she had a Telegram account, and the user responded "Of Course" (ofc) and provided the account name "tr3y8383." I know it is common for persons wanting to engage in communication about criminal conduct to obtain the Telegram account so they can move their conversation to a more private platform. On or about September 12, 2024, an FBI Portland Analyst searched "tr3y8383" in Telegram and located an account. Investigators have been unable to locate a specific Telegram account for MORENO, despite attempting to search Telegram by his known phone numbers. However, for the reasons stated above and the investigation to date, I believe MORENO operates a Telegram account that is currently unknown to investigators.

¹⁸ The "Target" is a number assigned to the username and provided in Instagram's records.

88. I reviewed records from Robinhood Markets, Inc. (“Robinhood”) for the account I believe was used by MORENO. Robinhood provides an electronic trading platform that facilitates commission-free trades of cryptocurrency, as well as cryptocurrency wallets and other features. The Robinhood account listed MORENO’s name, date of birth, social security number, and the email drugcoast@gmail.com, which I know to be used by MORENO. Robinhood’s records identified multiple “Crypto orders” in December 2023 and February 2024. Robinhood provided Crypto-specific statements that did not show a balance until December 2023, when it closed with \$93.22. The balance was \$113.57 by February 2024.

DEL CARPIO’s Use of Telegram and Cryptocurrency

89. While reviewing DEL CARPIO’s iCloud account I observed two phone numbers saved as “Telegram” phone numbers. The two numbers had “Jahzi 2x” and “Savior” as their respective contact names and were both previously on the same phone account plan as DEL CARPIO-0534. I believe both numbers were used by DEL CARPIO’s brothers (Jahzi and Savior Del Carpio, respectively). An FBI Portland Analyst attempted to search both numbers in Telegram but returned no results.

90. I also observed a chat between DEL CARPIO and the contact “Sean” in December 2023. During the chat, Sean asked DEL CARPIO “Can you load bit for me?” to which DEL CARPIO responded “Tele[.]” Sean responded, “Bet can you

hit me” and DEL CARPIO asked, “What’s your thing[,]” to which Sean responded “@ftoman83[.]” On or about September 12, 2024, an FBI Portland Analyst searched “ftoman83” in Telegram and did not locate an account. Investigators have been unable to locate a specific Telegram account for DEL CARPIO, despite attempting to search Telegram by his known phone numbers. However, for the reasons stated above and the investigation to date, I believe DEL CARPIO operates a Telegram account that is currently unknown to investigators.

91. I reviewed records from Block, Inc. (“Block”), for the account I believe was used by DEL CARPIO. Block’s portfolio includes CashApp, which offers investing in BTC, among other features. Block provided an image of DEL CARPIO’s driver’s license and verified his date of birth and social security number. The records were produced on or around March 22, 2024, and identified at least six BTC transactions between approximately July 14, 2023, and February 10, 2024. The transactions appeared to be internal currency exchanges between BTC and USD totaling over \$11,000 between them. There were also six external cryptocurrency addresses associated with the account.

REVES’ Use of Telegram and Cryptocurrency

92. While reviewing REVES’ iCloud account, there was a chat between his email account (jrsreves@gmail.com) and a contact saved as “J” in December 2023. In summary, REVES told J that he was going to call “jit today” who REVES described as “Dude from Tele with good prices[.]” J responded by sending REVES a

voice recording during which he told REVES “I know you talkin about Tele, but you know how many niggas you tellin me about some Telegram nigga? That’s what I’m tryin to figure out, like who is you talkin about?” (or something similar). I believe this conversation between REVES and J corroborates the use of “Tele” as an abbreviation for Telegram, as well as REVES’ active use of it to communicate with others. It should be noted that based on open-source research, I know “tele” can also be used as an abbreviation for other words (*e.g.*, hotel), which I believe the **Target Suspects** may use it for at times as well.

93. I similarly observed a chat in REVES’ iCloud between the **REVES Cell Phone** and the contact “Jahzi” who I believe to be Jahzi Del Carpio. The chat occurred on November 5, 2023. During the chat, REVES asked if Jahzi could send him “sum coin got the bread for u tn[.]” I know “coin” to be common shorthand for cryptocurrency and believe REVES was requesting payment via cryptocurrency in exchange for whatever the “bread” was he had for Jahzi “tonight” (tn). Jahzi responded with, “Yea send on tele[.]”

94. While reviewing REVES’ Instagram account (username “_jrreee” and Target 10753070868), I observed a conversation between REVES and the Instagram user “ballinassavie” (Target 44931733984). On or around January 7, 2024, REVES asked, “Yo u got a tele I can hit u on we can make bread together lmk my tele lurkin if you interested[.]” Based on my training and experience I know to “make bread” is a common reference to making money. I believe REVES was asking this user about

starting a conversation on Telegram during which they would discuss ways to make money together. Investigators have been unable to locate a specific Telegram account for REVES, despite attempting to search Telegram by his known phone number. However, for the reasons stated above and the investigation to date, I believe REVES operates a Telegram account that is currently unknown to investigators.

95. While reviewing REVES' iCloud I observed a December 2023 chat during which REVES made the following comments: "Yo put money in btc fam it's goin up[...]Made almost 1k sense last nigh[...]Put 150 in I promise you'll make bread[.]" I believe this corroborates REVES' investment in cryptocurrency like BTC.

CORDOVA's Use of WhatsApp and Cryptocurrency

96. An FBI Portland Analyst attempted to locate a Telegram account used by CORDOVA, or evidence of CORDOVA's use of Telegram, but was unable to as of September 9, 2024. However, the Analyst did locate a WhatsApp account associated with the **CORDOVA Cell Phone**. Based on my training and experience, I know WhatsApp is an encrypted communication platform. Like Telegram, WhatsApp's encryption makes it is very difficult for law enforcement to gain access to its content without access to the associated physical device. Based on my belief that CORDOVA's co-conspirators use Telegram, and the demonstrated association between CORDOVA and at least one encrypted communication platform (WhatsApp), I believe it is reasonable that CORDOVA likewise has a Telegram account that is currently unknown.

97. I also reviewed records from Block for the account I believe was used by CORDOVA. Block verified CORDOVA's government identification and provided an image of his driver's license. The account was also linked to CORDOVA-1128 and CORDOVA's Email. The records were produced on or around March 22, 2024, and identified twelve BTC transactions between approximately December 2, 2023, and February 5, 2024. The transactions appeared to be internal currency exchanges between BTC and USD totaling over \$6,000 between them. There were also 12 external cryptocurrency addresses associated with the account.

98. I reviewed records from Coinbase Global Inc. ("Coinbase"), a company that operates a cryptocurrency exchange platform, for the account I believe was used by CORDOVA. Coinbase provided an image of CORDOVA's driver's license and the account listed CORDOVA's name, date of birth, and social security number. The account was created in April 2021 and its listed phone number and email were the **CORDOVA Cell Phone** and CORDOVA's Email. Coinbase records showed CORDOVA created a BTC wallet in June 2022. Coinbase showed approximately 23 transactions between April 2021 and June 2021.

99. In addition to my training and experience, and the statements made by D.J.J. (as detailed above), I believe the foregoing corroborates my belief that some or all of the **Target Suspects** use Telegram (and/or other encrypted communication platforms) and cryptocurrency. I believe they likely use Telegram to communicate more openly about criminal activity. I therefore believe it is reasonable that their

encrypted communication platforms (in addition to unencrypted platforms) will contain evidence of their planning, coordinating, and executing the Target Offenses. I also believe their possession of cryptocurrency and virtual wallets may assist law enforcement with tracing the cryptocurrency that I believe was taken from D.J.J.

100. I know communication platforms like Telegram, and applications used to access virtual wallets, are stored on electronic devices like the **Target Devices**. I believe these **Target Devices** are typically stored in secure locations like on the owner's person, in their residence, or in their vehicle. As such, I will now establish each **Target Suspects'** current residence, cell phone, and vehicle (when applicable), where I believe such evidence will be found.

F. CORDOVA (SUSPECT 1): CELL PHONE, VEHICLE, LOCATION

CORDOVA's Transition from CORDOVA-1128 to the CORDOVA Cell Phone

101. On June 7, 2024, Judge Russo signed a search warrant (3:24-mc-623 B) authorizing the collection of historic and prospective geolocation data from CORDOVA-1128, serviced by AT&T. The affidavit supporting that application established probable cause that CORDOVA was the user of CORDOVA-1128. I reviewed CORDOVA-1128's historic location information between March 10, 2024, and June 6, 2024, and believe it was consistent with CORDOVA-1128 frequenting or residing at two locations, which included 20 Blackwell Pl, Palm Coast, Florida ("**CORDOVA Residence**"). However, based on my review of the records, I did not observe location information after approximately June 6, 2024. I also did not observe

toll activity (text and/or attempted voice calls) after June 10, 2024. On June 17, 2024, AT&T reported they cancelled the geolocation collection because CORDOVA-1128 was removed from their system on or about June 14, 2024. As detailed below, I believe that was the day CORDOVA-1128 transferred Providers from AT&T to Verizon (i.e., the **CORDOVA Cell Phone**); but I believe CORDOVA continued to use the same number. For clarity I will continue to refer to 904-674-1128 as CORDOVA-1128 while it was serviced by AT&T and as **CORDOVA Cell Phone** while serviced by Verizon.

102. On July 11, 2024, Judge Beckerman signed a warrant (3:24-mc-720) authorizing the collection of historic and prospective location information from the **CORDOVA Cell Phone**. The affidavit supporting that application established probable cause that CORDOVA continued to use the **CORDOVA Cell Phone** after it transferred Providers from AT&T to Verizon. This conclusion was based in part on: (1) Overlapping subscriber information (e.g., the subscriber name, home phone number, and email); (2) Toll analysis between CORDOVA-1128 and the **CORDOVA Cell Phone**; and (3) A July 10, 2024,¹⁹ search of the **CORDOVA Cell Phone** in CashApp which showed the associated display name “Billy Cordova” and username (i.e., “CashTag”) “\$Billyloco7.”

Identification of the CORDOVA Residence

¹⁹ In the aforementioned affidavit (3:24-mc-720) I mistakenly listed the date I searched CashApp as June 10, 2024. I will correct this in any affidavits going forward.

103. I queried CORDOVA's name and date of birth in a subscription-based, open-source database and observed the **CORDOVA Residence** was the most recently associated residence (last reported on November 30, 2023).

104. Based on records from Florida Power and Light ("FPL"), the listed customer at the **CORDOVA Residence** was Jordan Munoz ("Munoz"). Based on the investigation to date, I believe Munoz to be an associate of CORDOVA's. Both CORDOVA-1128 and the **CORDOVA Cell Phone** had numerous contacts with the phone number I believe was used by Munoz. There was also at least one group chat I observed in the aforementioned iCloud accounts which included both CORDOVA and Munoz, in addition to the January 6, 2024, image detailed above which captured the **Target Suspects** along with Munoz. Based on the details below, I believe CORDOVA resides at the **CORDOVA Residence** with Munoz.

105. On July 3, 2024, Judge Armistead signed an order authorizing the installation and use of a pen register and trap and trace device ("PRTT") on CORDOVA's Email. I subsequently obtained customer/subscriber records from Charter Communications Inc. ("Charter") for two IP addresses used by CORDOVA's Email on July 10, 2024, and August 6, 2024 (obtained pursuant to the PRTT). I also obtained records from Charter for a single IP address used by a Discord account associated with CORDOVA. Discord is an instant messaging and VoIP social platform, and the IP address was used on June 17, 2024. According to Charter's records, the listed subscriber for all three IP addresses was Alexis Kraemer

and the service address was the **CORDOVA Residence**. Around the time that the July 10, 2024, and August 6, 2024, IP addresses were used, location information for the **CORDOVA Cell Phone** was consistent with being in the vicinity of the **CORDOVA Residence**. In addition, I frequently observed a White Jeep bearing Florida license plate RKKA92 parked at the **CORDOVA Residence**. The Jeep was registered to Alexis Bauder, who is also known as Alexis Kraemer according to queries of a subscription-based open-source database.

106. I also reviewed multiple emails obtained from CORDOVA's Email records. One email included a gym membership application dated November 27, 2023, which listed the **CORDOVA Residence** as his address. A second email, dated December 28, 2023, thanked CORDOVA for his one-time payment to FPL, and listed the **CORDOVA Residence** as CORDOVA's address.

Surveillance Observations (Video and Cellular) at the CORDOVA Residence

107. On June 20, 2024, an FBI Jacksonville Special Agent observed a 1998 Silver Honda Civic bearing Florida license plate IQ13HJ, parked in the driveway connected to the **CORDOVA Residence**. According to Florida DMV records, CORDOVA was the Registered Owner of this vehicle (VIN: 1HGEJ8147WL075628) which will be referred to hereinafter as the **CORDOVA Vehicle**. From July 2024, to early September 2024, one or more FBI Special Agents (hereinafter "investigators") conducted regular surveillance²⁰ in the vicinity of the

²⁰ Each of these observation times will be in PDT, though the actual activities occurred in EDT.

CORDOVA Residence, and updated me regarding the results. During that time, investigators regularly observed the **CORDOVA Vehicle** arrive at and depart from either the designated driveway or the cul-de-sac area immediately in front of the **CORDOVA Residence**. Investigators could not observe the individual inside the **CORDOVA Vehicle**, or observe the driver enter the **CORDOVA Residence**; however, beginning on or around July 12, 2024, **CORDOVA's** presence at the **CORDOVA Residence** and the arrival and departure of the **CORDOVA Vehicle**²¹ were regularly consistent with the arrival and departure of the **CORDOVA Cell Phone's** arrival and departure in the same vicinity.

108. For example, on July 12, 2024, while the **CORDOVA Cell Phone** appeared to be in the vicinity of the **CORDOVA Residence**, investigators observed an individual walk from the **CORDOVA Residence** driveway, into the cul-de-sac, in the view of the camera. I compared the image of this person to two of **CORDOVA's** driver's license photos and a December 2023 booking photo, and I believe it is the same person. I also observed what appeared to be a right forearm tattoo. Though the details of the tattoo could not be seen, the location of the tattoo was consistent with the tattoo photographed during **CORDOVA's** December 2023 booking. See the images below comparing two of **CORDOVA's** Driver's License photos, his

²¹ Investigators could not always read the license plate clearly, but I will refer to each car that I believe matched the **CORDOVA Vehicle** (e.g., the color, make, and model) as such hereinafter.

December 2023 booking photos, and a still image from the July 12, 2024, surveillance:



109. On July 15, 2024, investigators observed the **CORDOVA Vehicle** arrive at the **CORDOVA Residence** around 11:33 a.m., pulling into the driveway connected to the **CORDOVA Residence**. The **CORDOVA Vehicle** departed again around 3:17 p.m. and returned around 3:41 p.m. Both arrivals and departures were consistent with the **CORDOVA Cell Phone's** location information.

110. On July 25, 2024, while the **CORDOVA Cell Phone** was consistent with being in the vicinity of the **CORDOVA Residence**, investigators observed the **CORDOVA Vehicle** depart from the driveway connected to the **CORDOVA Residence** around 1:58 p.m. Investigators could not see the driver, but the departure was consistent with the **CORDOVA Cell Phone**. Around the same time, investigators also conducted surveillance in the vicinity of 57 White Star Dr., Palm Coast, Florida ("White Star") and observed the **CORDOVA Vehicle** arrive at White Star around 2:24 p.m., consistent with the arrival of the **CORDOVA Cell Phone**. An individual I believe was consistent with CORDOVA exited the **CORDOVA Vehicle** and appeared to enter the residence. Around 4:08 p.m. what appeared to be the same individual exited the residence, entered the **CORDOVA Vehicle**, and departed, consistent with the **CORDOVA Cell Phone**. Investigators then observed the **CORDOVA Vehicle** return and park in the driveway of the **CORDOVA Residence** around 4:25 p.m.

111. On July 29, 2024, while the **CORDOVA Cell Phone** was consistent with being in the vicinity of the **CORDOVA Residence**, investigators observed an individual walk from the **CORDOVA Residence** driveway, into the cul-de-sac, in the view of the camera. The individual was consistent with CORDOVA and, based on the reasons detailed below, I believe he was CORDOVA. CORDOVA walked from the driveway in front of the **CORDOVA Residence** and entered the view of the camera around 3:44 p.m. He entered a red sedan as the passenger and departed

Affidavit of Jaron T. Cookson

around 4:27 p.m. The red sedan returned around 4:56 p.m. and CORDOVA exited the passenger seat and walked toward the **CORDOVA Residence**. CORDOVA returned to the view of the camera around 5:32 p.m. About two minutes later, the red sedan departed without him, and CORDOVA walked toward the **CORDOVA Residence**. CORDOVA's arrival, departure, and presence at the **CORDOVA Residence** were all consistent with the general location of **CORDOVA Cell Phone** at those times.

112. I also compared images of CORDOVA, captured through surveillance, to images provided to me by an FBI Portland Analyst, which he found on a publicly accessible Facebook account that I believe was used by CORDOVA. The account's display name was "Billy CORDOVA" and, based on records provided by Meta Platforms, Inc., which owns Facebook, the account's verified phone number and email were the **CORDOVA Cell Phone** number and CORDOVA's Email. This Facebook account had images of a person I believe was CORDOVA but without facial hair. See the images below comparing two Facebook images of CORDOVA—one with braids (dated July 26, 2022, and similar to his aforementioned booking photo) and one without braids (dated March 1, 2021)—to a still image from the July 29, 2024, surveillance:



113. Investigators continued to observe the **CORDOVA Vehicle** depart from or return to the **CORDOVA Residence** at times consistent with the **CORDOVA Cell Phone** through August 24, 2024, shortly after which the warrant authorizing the collection of location information from the **CORDOVA Cell Phone** expired.

114. On September 12, 2024, Judge Armistead signed a warrant authorizing the renewed collection of location information from the **CORDOVA Cell Phone**. I started receiving geolocation information for the **CORDOVA Cell Phone** on or about September 12, 2024, which remains active. That evening, the **CORDOVA Cell Phone** appeared to be in the vicinity of the **CORDOVA Residence** overnight.

115. Based on my observations of location information generated by the **CORDOVA Cell Phone** at times that I believe CORDOVA was at the **CORDOVA Residence**, I believe the location information generated by the **CORDOVA Cell**

Phone was consistent with CORDOVA being at the **CORDOVA Residence** for large portions of most days and regularly overnight. I believe this pattern was consistent with the user of the phone (i.e., CORDOVA) residing at the **CORDOVA Residence**. Based on the foregoing, I believe CORDOVA resides at the **CORDOVA Residence**, uses the **CORDOVA Cell Phone**, and regularly drives the **CORDOVA Vehicle**. I therefore believe CORDOVA's electronic devices, which I believe constitute evidence of the Target Offenses, may reasonably be found in each of these locations.

G. MORENO (SUSPECT 2): VEHICLE, LOCATION, CELL PHONE

Identification of MORENO-2316, MORENO Vehicle, and Prior Residence

116. As stated above, Verizon records showed MORENO-5756 (used at the time of the Target Offenses) was disconnected on March 29, 2024. In addition to MORENO-5756, I believe MORENO used the cell phone assigned the call number 929-501-2316 ("MORENO-2316") beginning at least as early as December 2, 2023, with service ending on or around August 7, 2024. On June 7, 2024, Judge Russo signed a warrant authorizing the collection of historic and prospective location information from MORENO-2316 (3:24-mc-623 D²²). The affidavit supporting that application established probable cause that MORENO was the operator of MORENO-2316, which was based in part on prior Spirit airline records; queries of a

²² An extension was signed by the Honorable John Jelderks, United State Magistrate Judge, District of Oregon, on July 18, 2024.

subscription-based open-source database; and toll analysis. It was noted in that supporting affidavit that certain details, such as toll records showing MORENO-5756 and MORENO-2316 contacted each other multiple times, indicated it was possible that MORENO-2316 and/or MORENO-5756 were used by someone other than MORENO at certain periods while both phones were active. However, as stated in that affidavit, and as supported by the details below, that does not change my belief that MORENO used MORENO-2316.

117. I received geolocation information for MORENO-2316 from approximately June 10, 2024, to approximately August 8, 2024. T-Mobile subsequently notified the FBI that they suspended MORENO-2316 on or around August 7, 2024. Based on my review, I believe the location information generated by MORENO-2316 regularly placed MORENO in the vicinity of 1851 LPGA Boulevard, Apt. 1206, Daytona Beach, Florida ("Apartment 1206"). I queried MORENO's name and date of birth in a subscription-based open-source database and discovered MORENO was previously associated with Apartment 1206.

118. Apartment 1206 was managed by the West Shore 500 East LLC ("500 East"). Based on 500 East's records, MORENO was one of two residents listed on the lease for Apartment 1206; the other was Adrianna Grammer ("Grammer"). Records from a subscription-based open-source database listed multiple aliases for Grammer, one of which was Adrianna Moreno. The same records also listed MORENO as Grammer's relative. I believe Grammer is MORENO's mother,

relative, or guardian. MORENO was scheduled to move in on July 20, 2023, and move out on August 19, 2024. Based on records from FPL, MORENO was the listed customer at Apartment 1206 and MORENO-2316 was the listed phone number for the FPL account.

119. According to the Florida Driver and Vehicle Information Database (DAVID), MORENO was the Registered Owner of a 2020 white Dodge Charger bearing Florida license plate 25BJAN, VIN: 2C3CDXH2LH186169 ("**MORENO Vehicle**"). Investigators conducted surveillance at Apartment 1206 for multiple periods between June 14, 2024, and August 19, 2024 (the date MORENO was scheduled to move out). During that time, investigators observed someone I believe was MORENO, the **MORENO Vehicle**, or both in the parking lot in front of Apartment 1206. Due to the placement of Apartment 1206, investigators could only see the parking lot and stairwell that can be used to access Apartment 1206, but not the unit's actual door. These observations were also frequently consistent with the location information generated by MORENO-2316 (prior to its suspension).

120. For example, on July 3, 2024, investigators conducted surveillance in front of the building connected to Apartment 1206. At approximately 11:17 a.m.²³ an individual that I believe was MORENO exited the apartment building. I knew from past surveillance that MORENO previously parked the **MORENO Vehicle** in the parking lot used by Apartment 1206 and its surrounding buildings. The presence of

²³ Each of these observation times will be in PDT, though the actual activities occurred in EDT.
Affidavit of Jaron T. Cookson

MORENO at Apartment 1206 prior to 11:17 a.m., and his suspected departure around that time, was consistent with MORENO-2316's geolocation information. See below for an image from surveillance compared to the images MORENO provided while making his Turo reservation.



121. Investigators also conducted regular surveillance at 13 Blaine Dr, Palm Coast, Florida ("13 Blaine"). On multiple occasions, investigators observed an individual I believe was MORENO arrive at and depart from 13 Blaine while driving the **MORENO Vehicle**, and at times consistent with the arrival and departure of MORENO-2316. For example, on August 2, 2024, at approximately 12:42 p.m., MORENO arrived at 13 Blaine Dr, Palm Coast, Florida ("13 Blaine") in the **MORENO Vehicle** at a time consistent with the arrival of MORENO-2316. See an image below of MORENO's arrival in the **MORENO Vehicle**:



122. Investigators also conducted surveillance at Apartment 1206 between August 16, 2024, and August 18, 2024, after MORENO-2316 stopped producing location information. Investigators observed MORENO access the **MORENO Vehicle** from outside of Apartment 1206 at or around 12:21 p.m. on August 16, 2024. MORENO pulled what appeared to be moving boxes from the **MORENO Vehicle**. On August 17, 2024, investigators observed MORENO arrive at and eventually depart from Apartment 1206 while driving a U-Haul truck, consistent with moving out by August 19, 2024. On August 18, 2024, investigators observed MORENO depart Apartment 1206 around 12:08 p.m., while driving the **MORENO Vehicle**.

123. On August 19, 2024, 500 East confirmed MORENO moved out. MORENO reportedly did not have a mail forwarding address yet, but provided what he described as his mom's address, 5000 Yukon Dr, Unit 308, Palm Coast, Florida ("**MORENO Residence**").

MORENO Vehicle's Geolocation Device and the MORENO Residence
Affidavit of Jaron T. Cookson

Page 68

124. Based on the foregoing, I believe MORENO actively uses the **MORENO Vehicle**. I believe the **MORENO Vehicle** will be located where MORENO resides and/or frequents and will therefore be located where evidence of the Target Offenses exists.

125. On August 23, 2024, the Honorable Youlee Yim You, United States Magistrate Judge, District of Oregon, signed a search warrant (3:24-mc-868) authorizing the collection of historic and prospective geolocation information from a cellular device installed in the **MORENO Vehicle**. The affidavit supporting that application established probable cause that the cellular device was installed in the **MORENO Vehicle** and contained a unique identifier that allowed it to connect to a cellular network provider (i.e., AT&T), and interact in a manner similar to a cell phone on AT&T's network.

126. I started receiving geolocation information for the **MORENO Vehicle** on or around August 26, 2024, which remains active. Based on my review, I believe the historic and prospective location information generated by the **MORENO Vehicle** regularly placed the vehicle in the vicinity of the **MORENO Residence** for large portions of most days and frequently overnight from August 18, 2024, onward.

127. The **MORENO Residence** was managed by the Pointe Grand Palm Coast LLC ("Pointe Grand"). According to Pointe Grand's records, the **MORENO Residence** was leased to Grammer. MORENO was not listed on the **MORENO Residence** lease but was also not listed on any other lease at the Pointe Grand

complex. I believe this is consistent with MORENO telling the 500 East that he did not yet have a permanent residence, but they could send mail to his mother's address (i.e., the **MORENO Residence**).

128. On August 27, 2024, an FBI Jacksonville Special Agent observed the **MORENO Vehicle** parked directly in front of the apartment building used to access the **MORENO Residence**. Parked next to it was a vehicle registered to Grammer. On August 29, 2024, a Flagler County Sheriff's Office ("FCSO") Deputy observed the **MORENO Vehicle** parked in front of the **MORENO Residence**. On September 4, 2024, the same FBI Jacksonville Special Agent observed the **MORENO Vehicle** parked in front of the **MORENO Residence**. All three observations were consistent with location information generated by the **MORENO Vehicle**.

MORENO Cell Phone

129. On September 12, 2024, Judge Armistead signed a warrant authorizing the collection of location information from the Verizon phone number assigned call number 551-237-0371 ("**MORENO Cell Phone**"). The affidavit supporting that application established probable cause that the phone was used by MORENO beginning August 8, 2024, when the phone was activated (around the time MORENO-2316 was suspended). The affidavit was based primarily on a common call analysis conducted by an FBI Portland Analyst which compared MORENO-2316 to the **MORENO Cell Phone**.

130. I started receiving geolocation information for the **MORENO Cell Phone** on or around September 12, 2024, which remains active. Based on my review, I believe the **MORENO Cell Phone's** location information since September 12, 2024, was consistent with being in the vicinity of the **MORENO Residence** for large portions of multiple days and overnight.

131. Investigators conducted surveillance in the vicinity of the **MORENO Residence** between September 11 and September 13, 2024. On September 11, 2024, investigators observed MORENO walk from the stairwell used to access the **MORENO Residence** and enter the **MORENO Vehicle**. Later that the same day, investigators observed MORENO return to and walk up the stairwell in the direction of the **MORENO Residence**, though the actual doorway to the residence could not be seen. Based on the placard above the stairwell used to access the **MORENO Residence**, the **MORENO Residence** was one of 12 units directly accessed by that stairwell, and one of 8 units on either the second or third floor.

132. On September 13, 2024, investigators observed MORENO walk from the stairwell used to access the **MORENO Residence** and depart in the **MORENO Vehicle**. When the **MORENO Vehicle** returned, investigators observed MORENO walk up the same stairwell and directly to the door used to access the **MORENO Residence**. MORENO's arrival and departure were both consistent with the location of the **MORENO Cell Phone's** location.

133. Based on the foregoing, I believe MORENO resides at the **MORENO Residence**, uses the **MORENO Cell Phone**, and regularly drives the **MORENO Vehicle**. I therefore believe MORENO's electronic devices, which I believe constitute evidence of the Target Offenses, may reasonably be found in each of these locations.

H. DEL CARPIO (SUSPECT 3): VEHICLE, CELL PHONE, LOCATION
DEL CARPIO'S Previous Residence and Target Vehicle

134. I received geolocation information for DEL CARPIO-0534 from approximately June 10, 2024, to approximately July 30, 2024, pursuant to the aforementioned search warrant and an extension. Around July 31, 2024, Verizon notified the FBI that DEL CARPIO-0534 was deactivated on July 28, 2024. Based on my review of the location information, I believe the location information generated by DEL CARPIO-0534 was consistent with being in the vicinity of 37 Fernmill Ln, Palm Coast, Florida ("37 Fernmill") for large portions of most days and regularly overnight. I believe this pattern was consistent with the user of the phone (i.e., DEL CARPIO) residing at 37 Fernmill during that time since at least June 10, 2024. I believe this was subsequently corroborated by surveillance of 37 Fernmill.

135. The morning of June 24, 2024, an FCSO Deputy Corporal conducted surveillance in the vicinity of 37 Fernmill and observed a 2019 black Toyota Camry bearing Florida license plate QFKG23 (VIN: 4T1BZ1HK7KU026287) parked in the driveway ("**DEL CARPIO Vehicle**"). According to DAVID, the vehicle was

registered to DEL CARPIO and Shirley E Gutierrez (“Gutierrez”). According to the Oregon Law Enforcement Data Systems (“LEDS”), Gutierrez was also the registered owner of a vehicle I observed driven by Jahzi Del Carpio on multiple occasions and that is regularly parked in the driveway of a residence I know is associated with Jahzi Del Carpio and Savior Del Carpio.

136. In addition, the aforementioned arrest of CORDOVA in December 2023, followed a traffic stop of the **DEL CARPIO Vehicle** which DEL CARPIO was driving.

137. In July 2024, investigators conducted regular surveillance²⁴ in the vicinity of 37 Fernmill. Investigators could see the driveway and sidewalk to the front door, though the front door was not visible during surveillance. During that time, investigators regularly observed a vehicle that I believe was the **DEL CARPIO Vehicle**, though investigators could not observe the license plate. Investigators also observed an individual I believe was DEL CARPIO coming and going from the direction of 37 Fernmill’s front door in a manner consistent with residing there and investigators observed him regularly drive the **DEL CARPIO Vehicle**. The arrival and departure of DEL CARPIO at 37 Fernmill was regularly consistent with general location of DEL CARPIO-0534.

138. For example, on July 5, 2024, at approximately 11:24 a.m., investigators observed an individual I believe was DEL CARPIO walking down the

²⁴ Each of these observation times will be in PDT, though the actual activities occurred in EDT.
Affidavit of Jaron T. Cookson

sidewalk in a manner consistent with exiting 37 Fernmill and walking toward the driveway. Very soon after, investigators observed the **DEL CARPIO Vehicle** parked in the driveway; though investigators were unable to see whether DEL CARPIO entered it. At approximately 11:55 a.m., investigators confirmed the **DEL CARPIO Vehicle** was no longer in the driveway. The next day, investigators observed an individual I believe was DEL CARPIO enter the **DEL CARPIO Vehicle** at approximately 11:07 a.m. and depart at approximately 11:15 a.m. DEL CARPIO's presence at and departure from 37 Fernmill on both occasions were consistent with DEL CARPIO-0534's location information at those times. See below for an image from surveillance compared to the photos DEL CARPIO provided for his Turo reservation:



139. As mentioned above, investigators stopped receiving location information from Verizon for Del Carpio-0534 on or about July 30, 2024. On July

31, 2024, Verizon notified the FBI that Del Carpio-0534 was deactivated on July 28, 2024. Within a few days, investigators stopped observing DEL CARPIO or the **DEL CARPIO Vehicle** at 37 Fernmill.

DEL CARPIO's Cell Phone and Residence

140. On August 19, 2024, Judge You signed a warrant authorizing the collection of location information from the AT&T phone assigned the call number 386-986-6110 ("**DEL CARPIO Cell Phone**"). The affidavit supporting that application established probable cause that DEL CARPIO was the user of the **DEL CARPIO Cell Phone**. According to AT&T's records, the **DEL CARPIO Cell Phone's** listed financial liable party, billing party, and user was DEL CARPIO, and it was activated on August 2, 2024. The listed address was 6 Flemington Ln, Palm Coast, Florida ("**DEL CARPIO Residence**"); the same address listed for DEL CARPIO-0534. I started collecting location information on or about August 20, 2024, and received historic location dating back to August 2, 2024.

141. On August 28 and September 4, 2024, an FBI Jacksonville Special Agent conducted surveillance at the **DEL CARPIO Residence** at times consistent with the **DEL CARPIO Cell Phone** being in the same vicinity. On both three occasions, the **DEL CARPIO Vehicle** was parked at the **DEL CARPIO Residence**.

142. From approximately September 6 to September 13, 2024, investigators conducted regular surveillance in the vicinity of the **DEL CARPIO Residence**.

Investigators observed an individual I believe was DEL CARPIO, and the **DEL**

CARPIO Vehicle, arrive and depart from the **DEL CARPIO Residence** on multiple occasions consistent with the vicinity of the **DEL CARPIO Cell Phone's** location. I believe these observations, and the location information generated by the **DEL CARPIO Cell Phone** since August 20, 2024, was consistent with DEL CARPIO residing at the **DEL CARPIO Residence**.

143. Based on the foregoing, I believe DEL CARPIO resides at the **DEL CARPIO Residence**, uses the **DEL CARPIO Cell Phone**, and regularly drives the **DEL CARPIO Vehicle**. I therefore believe DEL CARPIO's electronic devices, which I believe constitute evidence of the Target Offenses, may reasonably be found in each of these locations.

I. **REVES (SUSPECT 4): CELL PHONE AND RESIDENCE**

REVES Cell Phone and Residence

144. As stated above, T-Mobile's records listed 116 Red Mill Dr, Palm Coast, Florida ("**REVES Residence**") as the **REVES Cell Phone** address while it was subscribed to both REVES and Ozlem Reves. I queried a subscription-based open-source database using REVES' name and date of birth and saw his most recently associated address was the **REVES Residence**, last reported on June 11, 2024. I also reviewed Amazon's records for an account linked to REVES based on his name and the **REVES Cell Phone**, which showed the **REVES Residence** as his most recently added billing address (created under REVES' name in August 2023 and under Thomas Reves' name in May 2019).

145. I received geolocation information for the **REVES Cell Phone**, pursuant to the foregoing search warrant, and a search warrant extension, from approximately June 10, 2024, through approximately August 31, 2024, at which time the warrant authorization expired. I also received historic location information from November 1, 2023, to November 20, 2023, and then from March 10, 2024, to approximately June 7, 2024.

146. The prospective location information, received starting on or around June 10, 2024, was consistent with the **REVES Cell Phone** being in the vicinity of the **REVES Residence** for large portions of most day and regularly overnight. I believe this pattern was consistent with the user of the phone (i.e., REVES) residing at the **REVES Residence**.

147. According to LEDS, one of the vehicles previously registered to Ozlem Reves at the **REVES Residence** was a black 2015 Chevrolet Camaro bearing Florida license plate QQGN53 ("REVES Camaro," which is not the object of this application but is included herein to support the identification of REVES). On June 28, 2024, an FCSO Corporal conducted surveillance in the vicinity of 13 Blaine when the **REVES Cell Phone** was consistent with being in the same vicinity. The Corporal observed the REVES Camaro parked in the driveway. I subsequently located an archived story from REVES' Instagram records (obtained pursuant to the aforementioned warrant) that depicted REVES standing in front of a black vehicle that was consistent with the REVES Camaro. The post was dated December 20,

2023. See an image of the REVES Camaro at 13 Blaine and the Instagram post below:



148. From July 2024 to early September 2024, investigators conducted regular surveillance in the vicinity of the **REVES Residence**. Between July 2 and July 5, 2024, investigators observed a vehicle consistent with the REVES Camaro parked in the driveway at the **REVES Residence**. During the same period, investigators observed an individual I believe was REVES drive the REVES Camaro²⁵ on multiple occasions, and his arrivals and departures were consistent with the vicinity of **REVES Cell Phone's** location. The distance of the surveillance made it difficult to clearly see the individual's face, but I believe his physical appearance,

²⁵ Investigators also observed at least one other person operate the Chevrolet Camaro that was not REVES.

build, and right arm tattoo were consistent with REVES. See an image below of REVES standing in front of the REVES Camaro, parked at the **REVES Residence**:



149. Investigators eventually stopped seeing the REVES Camaro at the **REVES Residence**, but continued to observe REVES there. For example, on July 8, 2024, investigators observed REVES depart from the **REVES Residence** in what looked like the **MORENO Vehicle**. He was taken to 13 Blaine where he and MORENO appeared to enter the residence. MORENO and REVES later departed 13 Blaine and it appeared MORENO dropped REVES off at the **REVES Residence** a short time later. Each arrival and departure was consistent with the **REVES Cell Phone**. See images below comparing the image of REVES at the Felida Store in Vancouver, WA, on November 11, 2023, to his Instagram post and surveillance at the **REVES Residence** and 13 Blaine:



150. I continued to review the arrival and departure of the **REVES Cell Phone** from the **REVES Residence** and compared it to surveillance observations through August 28, 2024. I believe my observations continued to corroborate that REVES resides at the **REVES Residence**.

151. It should also be noted that on or about August 24, 2024, geolocation information for the **DEL CARPIO Cell Phone** and the **REVES Cell Phone** appeared to travel south together until they reached Miami, Florida. Both phones remained in the vicinity of Miami, Florida until August 28, 2024, when they traveled back to Palm Coast, Florida, and appeared to stop at the **REVES Residence** before the **DEL CARPIO Cell Phone** traveled to the vicinity of the **DEL CARPIO Residence**.

152. Investigators conducting surveillance observed a vehicle consistent with the **DEL CARPIO Vehicle** arrive at the **REVES Residence** on August 24, 2024, between approximately 4:25 a.m. and 4:57 a.m. An individual I believe was REVES exited the **DEL CARPIO** vehicle, entered the **REVES Residence**, returned to the **DEL CARPIO Vehicle**, and departed. REVES' arrival and departure were consistent with the foregoing location information. The **REVES Cell Phone** then traveled to the vicinity of the **DEL CARPIO Residence**, shortly after which both the **DEL CARPIO Cell Phone** and **REVES Cell Phone** appeared to travel south toward Miami. On August 28, 2024, a vehicle consistent with the **DEL CARPIO Vehicle** dropped REVES off at the **REVES Residence** around 10:04 a.m., consistent with location information from both phones.

153. An FBI Portland Analyst sent me multiple videos posted by both REVES' Instagram and MORENO's Instagram. Based on his review, the Analyst believed the content and/or background of the videos were consistent with both REVES and MORENO being in Miami, Florida. The images of both REVES and MORENO were a higher resolution than the surveillance detailed above. In one of MORENO's videos he is in the backseat of a sedan with red interior seats. I compared this interior to the interior of the **DEL CARPIO Vehicle** captured by a body-worn camera during DEL CARPIO's December 2023 traffic stop and arrest. I believe the interior was consistent. Based on these observations, I believe DEL

CARPIO drove REVES and MORENO to Miami, Florida in the **DEL CARPIO Vehicle**, where they stayed for multiple nights.

154. Based on the foregoing, I believe REVES resides at the **REVES Residence** and uses the **REVES Cell Phone**. I therefore believe REVES' electronic devices, which I believe constitute evidence of the Target Offenses, may reasonably be found in both locations.

J. ELECTRONIC STORAGE, DEVICE INFORMATION, AND TELEGRAM

Computers, Electronic Storage, and Forensic Analysis

155. As described above and in Attachments B-1 through B-7, this application seeks permission to search for records, including encrypted communications, cryptocurrency, and/or other digital evidence of the Target Offenses, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B), for any **Target Devices** (as defined above) found in the **Target Residences** or **Target Vehicles** and for which additional evidence is obtained by investigators indicating that the device was operated and/or owned by one of the **Target Suspects**.

156. *Probable cause.* I submit that if a computer, storage medium, or other **Target Device** is found on the **Target Residences** or in the **Target Vehicles**, and additional evidence exists indicating it was operated and/or owned by one of the **Target Suspects**, there is probable cause to believe records relevant to this investigation will be stored on that computer, storage medium, or other **Target Device** for at least the following reasons:

- i. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- ii. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- iii. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- iv. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

152. *Forensic evidence.* As further described in Attachments B-1 through B-7, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium (i.e., **Target Device**) found at the **Target Residences** or in the **Target Vehicles**, and for which additional evidence exists it was used and/or owned by a **Target Suspect** because:

- i. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- ii. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and

durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data.

Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- iii. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- iv. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible

to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrants.

- v. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

153. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded

on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- i. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrants call for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrants can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- ii. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled

environment will allow its examination with the proper tools and knowledge.

- iii. Variety of forms of electronic media. Records sought under these warrants could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

154. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants, and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

155. The initial examination of the **Target Devices** searched pursuant to this warrant will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

156. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the **Target Devices** or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

157. If an examination is conducted, and it is determined that the **Target Devices** do not contain any data falling within the ambit of the warrant, the government will return the **Target Devices** to its owner within a reasonable period of time following the search and will seal any image of the **Target Devices**, absent further authorization from the Court.

158. The government may retain the **Target Devices** as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the **Target Devices** and/or the data contained therein.

159. The government will retain a forensic image of the **Target Devices** for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant

claims that the government avoided its obligations by destroying data or returning it to a third party.

160. *Biometric data to unlock cellular telephones.* As described in Attachments B-1 through B-7, I am requesting warrants that would permit, during the execution of the search warrants, to obtain from any **Target Suspects** (but not any other individuals present at the **Target Residences** at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any cellular telephone(s) requiring such biometric access that are subject to seizure pursuant to these warrants for which law enforcement has reasonable suspicion that the aforementioned person's physical biometric characteristics will unlock the cellular telephone(s).

161. Under the requested warrants, while attempting to unlock the cellular telephone by use of the compelled display of biometric characteristics pursuant to these warrants, law enforcement would not be authorized to demand that the aforementioned person state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the cellular telephone(s). Nor do the requested warrants authorize law enforcement to use the fact that the warrants allow law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However,

the voluntary disclosure of such information by the aforementioned person is permitted. To avoid confusion on that point, if agents in executing the warrants ask any of the aforementioned person for the password to any cellular telephone(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any cellular telephone(s), the agents will not state or otherwise imply that the warrants require the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

162. Under the requested warrants, if the **Target Suspects** refuse to allow law-enforcement agents to apply their biometric characteristics to any cellular telephone seized pursuant to these warrants in a manner consistent with the warrants, he will be ordered to appear before United States Magistrate Judge Monte C. Richardson in Jacksonville, Florida, to show cause why he should not be held in contempt for failing to comply with a valid court order.

163. Based on my training and experience, I know that people who conspire with others to engage in crimes of violence often use their cell phones and computers to capture and store images or video recordings of such activity – sometimes referred to as “trophy photos.” They also often share these images or video recordings with their co-conspirators using text messaging or other forms of communication on their cell phone or computer such as online social networking services. Similarly, they often coordinate their criminal activity via text messages or other written

communications that are carried out by and stored on their cell phone and/or computer. These communications, images, and video recordings can be evidence of a perpetrator's knowledge or intent of their participation in the criminal activity.

164. Based on my training and experience, I know that crimes carried out by more than one person often involve some amount of communication among those involved. This may involve working out details of and preparing to carry out a premeditated crime, or simply arranging to meet up someplace where an unplanned crime would later occur. Either way, I know from training and experience that cell phones, email, text messaging, or other forms of communication via cell phone and computer and are often used for this purpose and that a cell phone or computer recovered from a participant in such criminal activity often contains evidence of communication among accomplices.

165. Based the information described above, as well as my training and experience, I know that persons engaged in crimes of violence in order to obtain cryptocurrency can inadvertently store evidence of such activity on a computer or other data storage devices through Random Access Memory and file path information. It is also common to utilize storage devices to document proceeds by co-conspirators so that the proceeds generated can be distributed evenly. Further, I know based on case information that to send, receive, and process cryptocurrency transactions, the **Target Suspects** must use internal and external storage devices to keep and maintain digital wallets to store the accumulated cryptocurrency.

166. Based on my training and experience, I know that individuals usually carry their personal devices with them—cellular phones, tablets, and/or laptops—when traveling away from their residence. Indeed, federal agents may encounter the **Target Suspects** away from their **Target Residences** when they arrest him, and it is reasonable to believe that the **Target Suspects** will have their personal devices on them at that time.

Additional Details Regarding Cell Phones

167. Based on my training and experience, a cell phone is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; recording, storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet, including the use of apps. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

168. Based on my training, experience, and research, I know that cell phones have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, and GPS navigation device. In my training and experience, examining data stored on wireless telephones can uncover, among other things, evidence that reveals or suggests who possessed or used the phone, how the phone was used, the purpose of its use, and locations of evidentiary value to the investigation.

Remote Search for the Target Suspects' Telegram Account(s)

169. As stated above, based on my conversations with investigations experienced with investigating SIM swapping attacks, I know that individuals frequently use Telegram to communicate. I know that various public and private channels on Telegram are devoted to discussions about SIM swapping attacks where individuals discuss victims, methods, and attacks.

170. Based on the investigation to date, and my conversations with other investigators, I know that D.J.J. personally used Telegram and participated in these chats to discuss cryptocurrency theft. I also know D.J.J. has specifically used Telegram to communicate with subjects of other FBI investigations engaged in SIM swapping.

171. I have learned that Telegram (also known as "Telegram Messenger") is a mobile and desktop messaging application. It can be used on smartphones, such as

Apple iOS, and Google Android devices, and on desktop computers, by users to send messages and media to each other.

172. To sign up for a Telegram account, a user must provide a phone number. Telegram verifies the phone number through a text message sent to the phone number. Telegram users can also select a username but are not required to. Usernames are unique, meaning only one user can have a particular username. Telegram users can find other users by searching for the username or by using the known phone number of a user. Users can also select a display name, such as a first and last name. Display names are not unique.

173. Telegram offers a variety of communication methods for its users:

- i. **Chats.** Users on Telegram can communicate with each other through chats. They can send each other text messages, photos, videos, any files, and make voice calls.
- ii. **Secret Chats.** Secret chats use end-to-end encryption, which means only the sender and recipient have the ability to view the content of the chats. These secret chats also disappear and can be set to self-destruct.
- iii. **Groups.** Telegram allows collections of users to communicate with each other in chat rooms called groups. Groups may be invitation only.

174. According to Telegram's privacy policies, Telegram stores basic user account data, including mobile number, profile name, profile picture, screen names, and e-mail address, to the extent a user has provided this information.

175. Telegram also stores messages, photos, videos and documents from a user's chats and private messages, as well as from public channels and public groups in which the user participates.

176. Telegram also stores a user's contacts and can sync with the user's contacts on his device.

177. Telegram also can store cookies on a user's device that allow Telegram to provide and customize its services to the user.

178. Telegram states that it retains this data "for as long as it is necessary for us to fulfill our obligations in respect of the provision of the Services."

179. Telegram has advertised that it has over two hundred million active monthly users.

180. Based on my conversations with other investigators, I know that evidence of who was using a Telegram account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. The records and information described in Attachment B-8 represent the type of data expected to be located on the **Telegram Servers** based on information obtained from the **Target Devices**, based on my experience and that of other federal agents.

181. Based on my training and experience, if a Telegram user logs into his or her Telegram account from a new device, all of the user's previous activity on Telegram, including chats, messages in groups, etc., are available on the new device if the user did not previously delete it.

182. In some cases, electronic storage information such as chat content and Cloud-stored data may only be accessed over the Internet from an authorized device. Depending on the service being used, the actual location at which the electronically stored information is stored may be concealed through technological means such as encryption and distributed infrastructure. In these instances, it may be necessary for officers executing the search to use remote access from an authorized device, such as the **Target Device(s)**, to make a local copy of the electronically stored information. The copy can then be searched using the means outlined elsewhere in this affidavit.

183. This Court has jurisdiction to issue the requested warrant under Rule 41(b)(6)(A) because the below facts establish there is probable cause to believe that the district where the information is located has been concealed through technological means and that there is probable cause to believe that activities related to the crime being investigated occurred within this judicial district.

184. The locations of Telegram's data centers are not publicly disclosed, but IP addresses for datacenters or proxy services to reach data centers are made available by Telegram as part of the application programming interface ("API") used to interact with the Telegram network. Publicly available information obtained from

the Telegram API has identified U.S.-based IP addresses as access points to Telegram data centers, indicating that either a proxy service or the actual data center is located in the United States.

185. Telegram historically has refused to respond to legal process from the United States. According to Telegram's privacy policy, "If Telegram receives a court order that confirms you're a terror suspect, we may disclose your IP address and phone number to the relevant authorities. So far, this has never happened." Telegram further states:

To protect the data that is not covered by end-to-end encryption, Telegram uses a distributed infrastructure. Cloud chat data is stored in multiple data centers around the globe that are controlled by different legal entities spread across different jurisdictions. The relevant decryption keys are split into parts and are never kept in the same place as the data they protect. As a result, several court orders from different jurisdictions are required to force us to give up any data.

Thanks to this structure, we can ensure that no single government or block of like-minded countries can intrude on people's privacy and freedom of expression. Telegram can be forced to give up data only if an issue is grave and universal enough to pass the scrutiny of several different legal systems around the world.

To this day, we have disclosed 0 bytes of user data to third parties, including governments.

186. This perspective appears to come from Telegram's founder and CEO, Pavel Durov, who has tweeted, "We've no issue with formalities, but not a single byte of private data will ever be shared with any government." Telegram has repeatedly refused to provide records to the Department of Justice pursuant to U.S. legal process.

Affidavit of Jaron T. Cookson

Page 100

Good Cause for an Any Time Execution

187. I request authorization to execute the proposed search warrants at any time during the night or day, based on the following factors which demonstrate good cause: (1) the subjects are suspected of having committed a crime of violence have a violent criminal history; (2) investigators suspect the presence of firearm(s) at the locations to be searched; and (3) once the **Target Devices** described herein are in law enforcement's possession, the execution of the warrants authorizing their search will not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of these warrants at any time in the day or night.

CONCLUSION

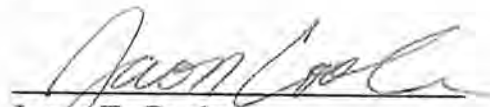
188. Based on the foregoing, I have probable cause to believe the Target Offenses were committed by the **Target Suspects**, and that evidence of these offenses, as more fully described in Attachments B-1 through B-8 hereto, is presently or will be located at the **Target Locations**, in the **Target Vehicles**, and on the **Telegram Servers**, which are described above and in Attachments A-1 through A-8. I therefore request that the Court issue a warrant authorizing a search of the **Target Residences**, **Target Vehicles**, and **Telegram Servers**, as described in Attachments A-1 through A-8, for the items listed in Attachment B-1 through B-8, and the seizure and examination of any such items found.

Request for Sealing

Affidavit of Jaron T. Cookson

Page 101

189. I further request that this Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search warrant, including the application, this affidavit, the attachments, and the requested search warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at this time may cause flight from prosecution, cause destruction of or tampering with evidence, cause intimidation of potential witnesses, or otherwise seriously jeopardize an investigation. Premature disclosure of the contents of the application, this affidavit, the attachments, and the requested search warrant may adversely affect the integrity of the investigation.


 Jaron T. Cookson
 Federal Bureau of Investigation

Subscribed and sworn before me this 23rd day of September, 2024.


 HONORABLE MONTE C. RICHARDSON
 United States Magistrate Judge

ATTACHMENT A-8

Electronically Stored Information to be Searched

The electronically stored information to be searched is any remotely accessible information stored at a location concealed through technological means and linked to any computer (as defined in Attachment B-8) that is: (1) found at a **Target Residence** or in a **Target Vehicle**, as described in Attachments A-1 through A-7; and (2) for which additional evidence exists that the computer was used by Billy CORDOVA, Ralph MORENO, Justice DEL CARPIO, or Jackson REVES; and (3) on which a Telegram account is located.

ATTACHMENT B-8**Items to Be Seized**

The items to be searched for, seized, and examined, are those located in the remotely-accessible electronic information (hereinafter “**Remote Data**”) as described in Attachment A-8, that contain evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 1201(c), Conspiracy to Kidnap; and 18 U.S.C. § 1201(a)(1), Kidnapping (hereinafter “Target Offenses”). The items to be seized cover the period of September 24, 2023, through the date of the execution of the search warrant.

A. The items referenced above to be searched for, seized, and examined are as follows:

1. All communications, records, documents, programs, applications or materials related to the planning, coordination, or completion of the kidnapping and/or extortion of the adult victim (“AV”) described in the affidavit supporting this warrant, in violation of the Subject Offenses.

2. All communications, records, documents, programs, applications or materials related to locations or identities of individuals involved in the Subject Offenses.

3. All communications that investigators believe is with or about AV, whether or not his/her true name is used.

4. Records and information containing photographs, videos, and/or audio recordings related to the Subject Offenses.

5. All communications, records, documents, programs, applications or materials related to bank accounts or cryptocurrency accounts/wallets used in furtherance of the Subject Offenses.

6. Records, communications, images, videos or audio recordings indicative of expenses paid and/or proceeds gained from carrying out the Subject Offenses (e.g., records of payments made to purchase airline tickets, cryptocurrency payments between suspected co-conspirators around the time of the Subject Offenses, wallet addresses associated with these transactions, etc.).

7. Financial records including bank statements, canceled checks, deposit records, check stubs, payment ledgers, checkbook registers, deposit slips, loans, documentation of assets and liabilities, general ledgers, general journals, cash, cash receipts, cash disbursement journals, accounts receivable journals, accounts payable journals, contracts, billing information, and records of bills relating to the receipt of currency, cryptocurrency, or other forms of payment.

8. Records relating to custody, control and ownership of account(s) and/or computer(s) used in the foregoing communication(s);

9. Cryptocurrency and related records or communications of any kind, including but not limited to:

- a. cryptocurrency hardware wallets, digital offline storage devices, cold storage devices, Mnemonic phrases, passwords, encryption keys and seed recovery lists;
- b. any and all representations of cryptocurrency public keys or addresses, whether in electronic or physical format;
- c. any and all representations of cryptocurrency private keys, whether in electronic or physical format;
- d. any and all representations of cryptocurrency wallets or their constitutive parts, whether in electronic or physical format, to include “recovery seeds” or “root keys” which may be used to regenerate a wallet.

10. The United States is authorized to seize any and all cryptocurrency by transferring the full account balance in each wallet to a public cryptocurrency address controlled by the United States

B. As used in this attachment, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage and any file format.

C. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical,

arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

C. During the execution of the search of the computers (as defined above) described in Attachment A-8 and located at the **Target Residences** (described in Attachments A-1 through A-4) or in the **Target Vehicles** (described in Attachment A-5 through A-7), law enforcement personnel are authorized to use remote access to search and to seize or copy the **Remote Data** if the district where the media or information is located has been concealed through technological means, such as Telegram data.

Search Procedure

A. The search for **Remote Data** capable of being reviewed by the government may require authorities to employ techniques, including linking additional government-controlled devices to Telegram account(s) or live downloading of electronically-stored information, that might result in minor alterations being made to the state of the **Remote Data** while it is recovered.

B. The initial examination of the **Remote Data** will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this

review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

C. If, at the conclusion of the examination, law enforcement personnel determine that particular files or communications stored in the **Remote Data** do not contain any information falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or communications falling within the purview of the warrant through the conclusion of the case.

D. The government will retain a full copy of the **Remote Data** for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.